\Orchestrating a brighter world NEC

Business ConneCT

Installation Guide

A publication of NEC Nederland B.V.

Date: April 12th 2021

Great care has been taken to ensure that the information contained in this document is accurate and complete. Should any errors or omissions be discovered or should any user wish to make a suggestion for improving this document, they are invited to send the relevant details to:

NEC Nederland B.V.
P.O. BOX 32
1200 JD Hilversum
The Netherlands

Disclaimer: Our products are subject to continuous development and improvement. Therefore additions or modifications to the products after mentioned date may cause changes to the technical and functional specifications. No rights can be derived from the contents of this document. NEC Unified Solutions and/or its respective suppliers make no representations about the suitability of the information contained in this document and related graphics published as part of the services for any purpose. This document and related graphics are provided "as is" without warranty of any kind. NEC Unified Solutions and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall NEC Nederland B.V. and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services. This document and related graphics published on the services could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. NEC Enterprise Solutions and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. The example companies, organizations, products, domain names, e-mail addresses, logos, people, places and telephone numbers depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place or telephone number is intended or should be inferred.

Models may vary for each country, and due to continuous improvements this specification is subject to change without notice. Please refer to your local NEC representative(s) for further details.

Business ConneCT 12.0
Installation Guide

PREFACE

This book describes how to install, configure and maintain Business ConneCT.

Business ConneCT is an all-in-one Unified Communication solution that provides Operator, Contact Center and Employee functionality on one server, using one database and a single user interface. This scalable, flexible and robust UC solution is ideally suited to meet the dynamic business communication needs of today. Business ConneCT supports all NEC's existing PBX platforms.

Changes to this Installation Guide compared to Business ConneCT version 11.1 are marked yellow. Note that if an entire chapter is new, only the chapter header will be marked yellow.

1. INTRODUCTION

BCT is a business telephony application. Based on user roles, it offers operators, Contact Center agents and employees all the functionality they need for effective communication.

- **Employee:** Modern office users expect more from their office communication solution and that is what BCT provides. Easy and complete directory access, call handling, presence management, voicemail, group display and availability information is all included in a single window interface.

- **Operators:** The operator application provides the complete functionality that an operator expects. Directory information, busy lamp field and easy call queuing and transfer are all available. Also for employees who temporarily have to fill in the operator position, the intuitive interface provides a very effective solution.

- **Contact Center agents:** BCT offers the most required Contact Center functionality. Starting with basic call routing for the typical small help desk environment to enhanced functionality like skill based routing, Email routing, Auto-attendant/IVR, caller identification and complete supervisor.

The key features of the BCT platform are:

- ✓ One server;
- ✓ One integrated database (see also ***Note 1***);
- ✓ One overall installation;
- ✓ One Point of Management & Point of entry;
- ✓ One User Interface for all roles.

If the customer wants to synchronize between BCT and for example MA4000, you need to install the Aranea add-on tool. This tool is available on the BCT product DVD. For information, please refer to the Aranea Installation and Configuration Guide.

The Configuration Wizard helps you to configure the application. This makes it much easier to configure Operator, Agent and Voicemail handling. The Configuration Wizard can also be used to make changes in the system when the system is configured via the Configuration Wizard. See section 8.1.1 Using the Configuration Wizard.

Note 1: *The default BCT SQL database name is "United". When a custom database name is defined during initial install of BCT the "United" database name as used throughout this document should be interpreted as the custom defined database name.*

Note 2: *In case the location of a file or directory is indicated, then this is specified for a 64-bit operating system environment (e.g. C:\Program Files (x86)\..). If you use a 32-bit environment, you need to use the corresponding location (C:\Program Files\..).*

1.1. References

BCT Administrator Guide	Can be found on D:\Business ConneCT Resources\Documentation\ BCT 12.00 - AdministratorGuide-EN.pdf
BCT Supervisor Guide	Can be found on D:\Business ConneCT Resources\Documentation\ BCT 12.00 - SupervisorGuide-EN.pdf
BCT User Guide	Is also available as On-Line Help. Right-click on the "?" icon of the Business ConneCT desktop client for the BCT-UserGuide-XX.pdf. (xx = language). File can also be found on D:\Business ConneCT Resources\Documentation\User Guides
Securing BCT Web Applications	Can be found on D:\Business ConneCT Resources\Documentation\White Papers
BCT Mobile Client Network Security	Can be found on D:\Business ConneCT Resources\Documentation\White Papers
Aranea Installation and Configuration Guide	Can be found on D:\Aranea 3.03\
BCT Boundary Specification	Can be found on D:\Business ConneCT Resources\Documentation We strongly advise you to use the latest version. Can be found on NEC BusinessNet – “Home > Products and Solutions > Unified Communications > Business ConneCT > Product Documents” (under ‘Service Manual’)

Note: *Locations above assume that* ***D:*** *is the drive letter related to DVD drive containing the BCT DVD.*

1.2. Abbreviations

ACD	Automatic Call Distribution	PBX feature
BCT	Business ConneCT	Product name
CCIS	Common Channel Interoffice Signaling	Inter PBC link
CLI	Calling Line Identification	Telephony feature
CSTA	Computer Supported Telephony Applications	Interface protocol
CSV	Comma Separated Values	File Format
CTI	Computer Telephony Interface	Interface type
DDI	Direct Dialing In (=DID)	Telephony feature
DID	Direct Inward Dialing (=DDI)	Telephony feature
DND	Do Not Disturb	Telephony feature
DAP	DECT Access Point	DECT interface
GUI	Graphical user Interface	Software layer
FCCS	Fusion Call Control System signaling	Inter PBC link
FCO	Field Change Order	Document
IE	Internet Explorer	Web browser
IVR	Interactive Voice Response	Voice application

MA	Mobility Access	PBX Feature
MAT	Maintenance Access Terminal	Interface protocol
ME	Mobile Extension	PBX Feature
NAT	Network Address Translation	IP address translation
NSIP	NEC Session Initiated Protocol	Terminal protocol
OAI	Open Application Interface	Interface protocol
OS	Operating System	Software layer
PBX	Private Branch Exchange	System
OWI	Open Web Interface	API protocol
PID	Personal Identification	Security key
PVE	Private Virtual extension	Interface protocol
PVM	Protected Virtual Machine	Software layer
RTP	Real-time Transfer Protocol	Interface Protocol
TAC	Trunk Access Code	Dialing rules concept
UCD	Uniform Call Distribution	PBX feature
UCS	Unified Contact Server	Software layer
UI	User Interface	Software layer
VM	Virtual Machine (A virtual PC not directly running on physical HW, but rather on a virtual HW layer provided by the Hypervisor)	Software layer
VMP	Voice Media Processing	Interface protocol
XPS	XML Paper Specification	Microsoft doc format

1.3. Installed components

This section summarizes the application shortcuts that are available after installation.

1.3.1. Server components

Business ConneCT

This is the main entry in the start menu of the server PC. It contains the next shortcuts:

- BCT Supervisor Dashboard – provides a graphical and user friendly interface for Administrator and Supervisor.

  To the Supervisor it provides a Dashboard, Monitors and Floorplans to view real-time contact center information. To the Administrator it provides a tool kit for building the Call Flow.

  The Administrator (or PBX engineer) also uses this tool to configure the system. Call Flows can be built by connecting standard modules. Several different Call Flow designs can be configured to run simultaneously and in parallel.
- BCT System Settings – for user management and general configuration of the system.
- Business ConneCT Client – a BCT server may also include BCT client. See below.

Documentation

This folder contains:

- BCT Administrator Guide
- BCT Supervisor Guide

Tools

This folder contains:

- Configuration Wizard – allows initial configuration of BCT for a stand-alone PBX with a single operator.
- Diag@Net Monitor – used to monitor trace files and set trace levels.
- Directory Import Formatter - validates a CSV file for having a BCT readable format which can be used for import via the Directory Import feature of BCT.
- License Manager – used to activate the licenses for BCT modules.
- Runtime Manager – BCT uses a service called UCS Runtime. You must start this service so that the Contact Center part of BCT may operate normally. The application to start BCT is called the Runtime Manager. In addition to that, a number of administrative tasks can be done with the Runtime Manager.
- Security Configurator – used to set the server security policies.
- System Health Status – displays the health status of various components of BCT.
- System Info Console – can be used to create an overview of the installed components and system settings.
- Configuration Manager – used to modify the values of keys in BCT configuration files.
- Server Manager – used for making database and settings backup and restore, to change BCT services SQL account credentials and repair secure port certificate bindings.

1.3.2. Client components

Business ConneCT

This is the main entry of the start menu on the client PC. It contains the next shortcuts:

- Business ConneCT Client **–** Used to start the BCT Desktop Client application on the PC.

Note: *BCT includes also BCT Essential Employee Client (web client) with essential functionality for the Employee. See 23 Appendix M – ESSENTIAL EMPLOYEE CLIENT INSTALLATION AND CONFIGURATION .*

- BCT Supervisor Dashboard **–** this is a Contact Center management and monitoring tool that can be installed on the client PC via the BCT Contact Center Client package from the product DVD.

Documentation

If the user is also administrator or supervisor of the Contact Center, then this folder will be available, and contains:

- BCT Administrator Guide
- BCT Supervisor Guide

1.4. Deployment view

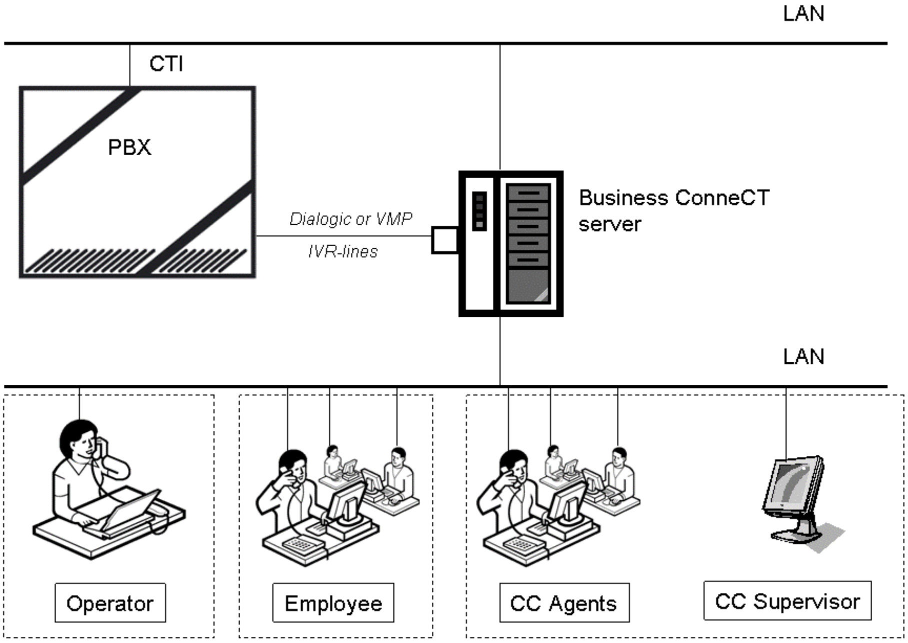


Figure 1-1 BCT overview

The BCT applications are available centrally on a server and distributed over the network to the clients. In the context of this document, clients are computers on which the BCT applications are used, i.e. the end user computers.

The following components are used in BCT:

- BCT Server Software
- BCT Client
- BCT uses the United database
- Client computers including web browsers
- Data network
- Database (server)

The CTI link is the licensed connection between the BCT server and the PBX. Both ends of the link need fixed IP addresses.

- For a SV8100/SV9100, AspireX/AspireUX, SV8300/SV9300 or SV8500/SV9500 - this is the OAI (/MAT) interface.
- For an SV9100-TAPI - this is the TAPI (3rd party CTI Driver) (/MAT) interface.
- For an iS3000 / SIP@Net - this is the CSTA (/PVE) interface.
- For UNIVERGE 3C - this is the SOAP Web Service Interface.

Note: The main difference between (SV8100)/SV9100 and SV9100-TAPI is the usage of OAI versus TAPI (3rd party CTI driver). Where (PBX/Business ConneCT) configuration is identical for both types SV8100/SV9100 is indicated in this document. For explicit differences, SV9100-TAPI is indicated separately. In certain geographical regions only TAPI is supported for SV9100.

1.5. Licensing

The following figure shows the BCT licenses and the valid combinations.

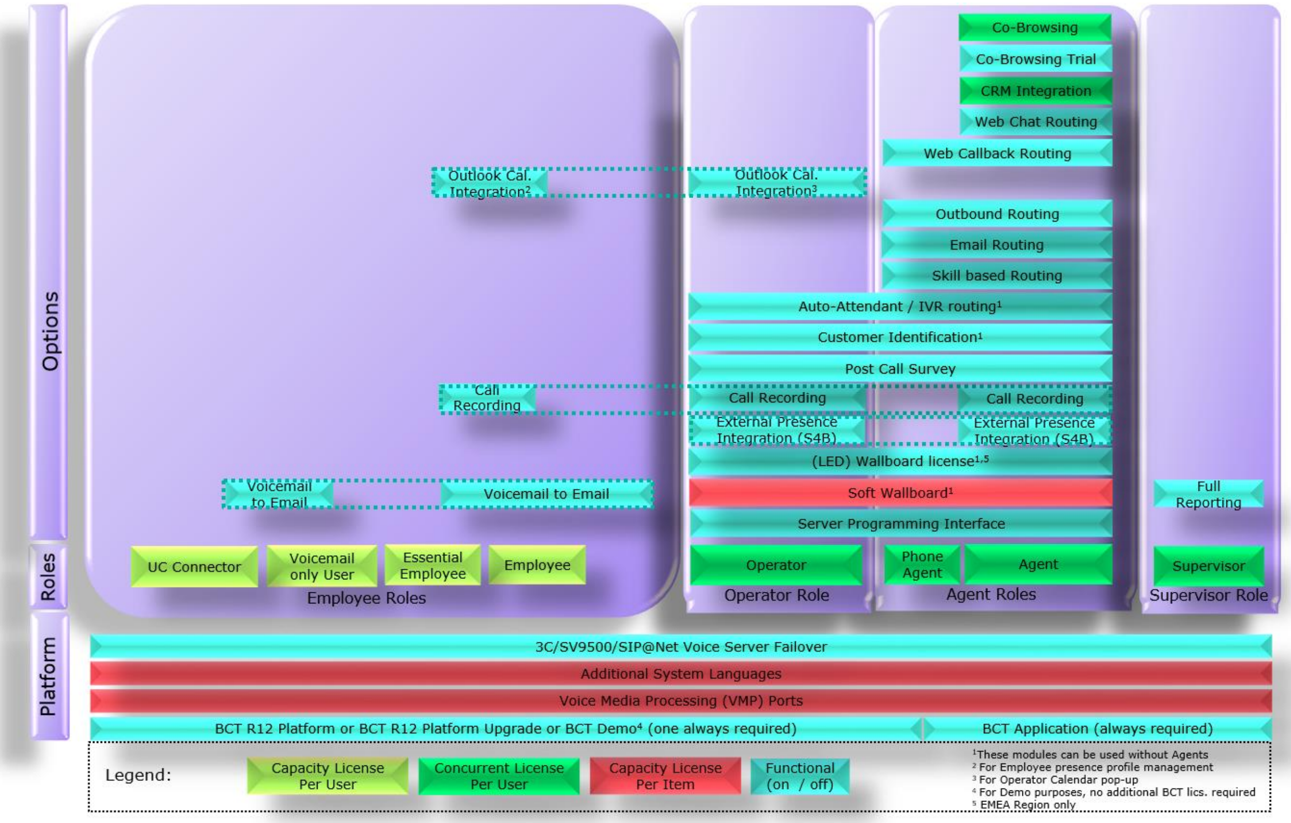

Options
Roles
Platform
Co-Browsing
Co-Browsing Trial
CRM Integration
Web Chat Routing
Web Callback Routing
Outlook Cal. Integration²
Outlook Cal. Integration³
Outbound Routing
Email Routing
Skill based Routing
Auto-Attendant / IVR routing¹
Customer Identification¹
Post Call Survey
Call Recording
Call Recording
Call Recording
External Presence Integration (S4B)
External Presence Integration (S4B)
(LED) Wallboard license¹·⁵
Voicemail to Email
Voicemail to Email
Soft Wallboard¹
Full Reporting
Server Programming Interface
UC Connector
Voicemail only User
Essential Employee
Employee
Employee Roles
Operator
Operator Role
Phone Agent
Agent
Agent Roles
Supervisor
Supervisor Role
3C/SV9500/SIP@Net Voice Server Failover
Additional System Languages
Voice Media Processing (VMP) Ports
BCT R12 Platform or BCT R12 Platform Upgrade or BCT Demo⁴ (one always required)
BCT Application (always required)
Legend:
Capacity License Per User
Concurrent License Per User
Capacity License Per Item
Functional (on / off)
¹These modules can be used without Agents
² For Employee presence profile management
³ For Operator Calendar pop-up
⁴ For Demo purposes, no additional BCT lics. required
⁵ EMEA Region only

Figure 1-2 BCT license structure

There are four types of licenses:

Functional licenses

They enable a feature. This license category comprises all options.

Capacity based licenses

They are calculated per user or per item. This category comprises all user roles, the additional system languages and the VMP ports. Capacity based licenses can be static or concurrent. Employee licenses are static; this means that the license is associated with one specific user. Operator, Agent and Supervisor licenses are concurrent licenses. This means that any number of users can be assigned access to these roles. The license is claimed as soon as a user logs in as Operator, Agent or Supervisor. Additional system languages are also concurrent; they are claimed when the system administrator makes them available to users.

Demo license

This is a special license intended for demonstration systems only. Whenever the system is loaded with the demo license it will give you a fixed set of functionality and limited call handling performance (only 6 concurrent calls are supported under the Demo License). When the system is running with a Demo License, this can be verified in the following ways:

- System Health will show “Demo System”.
- BCT Desktop Client will show "Business ConneCT - Demo System - xxxx" in the title bar.

- The license manager will show a functional license called "Demo System".
- Diag@Net (diagnostics) tracing will show trace lines with text "Setting product in Demo Mode".

Free trial License
See 1.5.1 Free Trial mode.

1.5.1. Free Trial mode

Preconditions

1. The available 90 days of free trial have not been used.

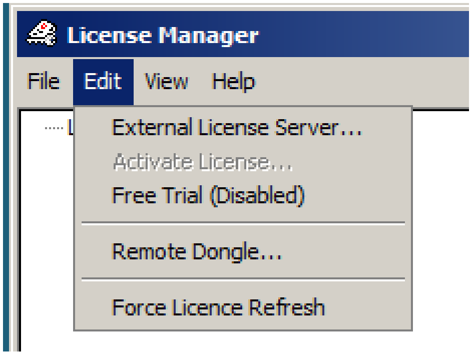
What is Free Trial mode?

- BCT has a free trial mode. In this mode the BCT system will function without licenses. The system is fully functional (within regular BCT boundaries) and can be used for 90 days. After this period the system will stop working or fall back to the license that was active before enabling the free trial mode.
- Free trial mode can be used for demo and testing purposes and when the regular / commercial license is not operational (i.e. wrong license ordered etc.).
- All BCT desktop clients will show in their title bar that the system is in free trial mode.
- 7 days before the free trial mode expires, the system health page will indicate that there are 7 (or less) days of free trial mode left.
- The free trial mode can be activated in the BCT Configuration wizard (see 8.1.1 Using the Configuration Wizard) and in the license manager.

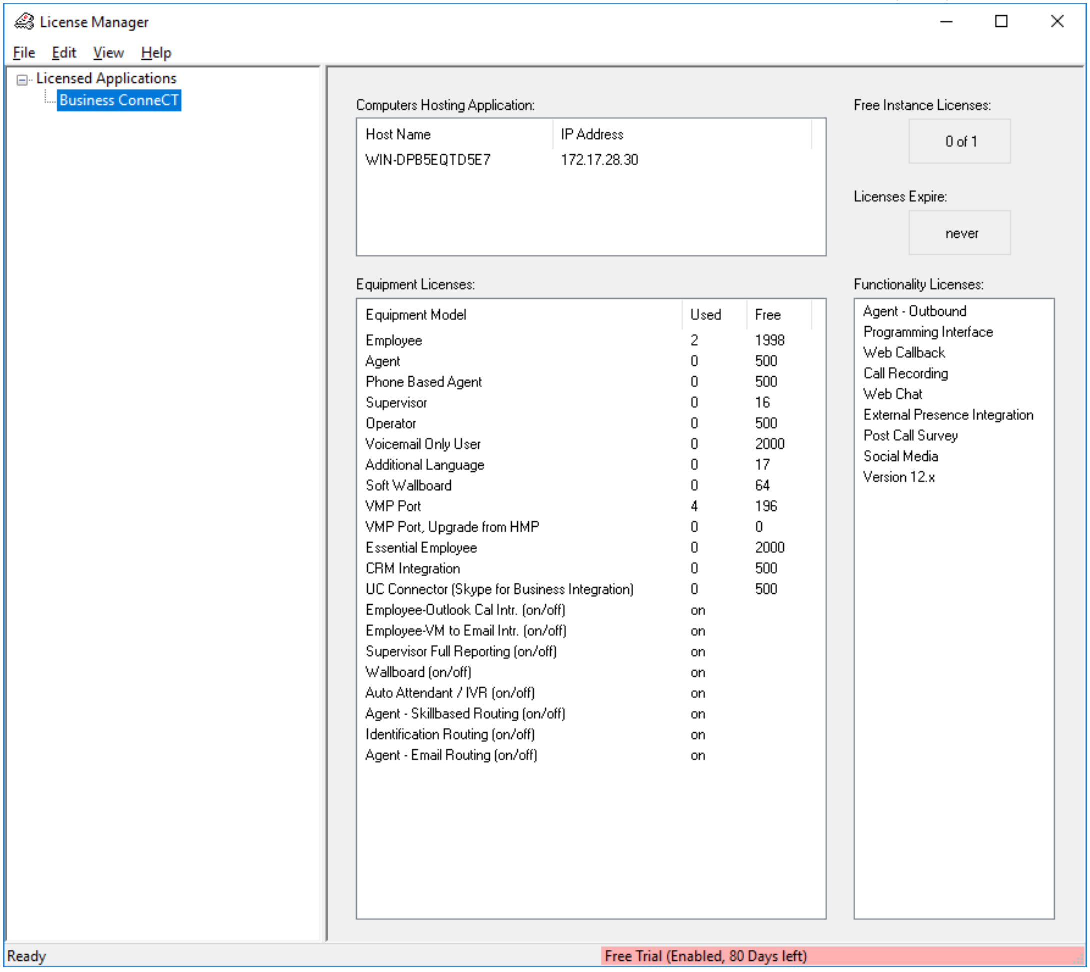
Steps to activate in the BCT License Manager
Applies to SV8100 / SV9100 or Univerge 3C only.

1. Start the License Manager via **Start-Menu > Programs > Business ConneCT > Tools > License Manager**.

2. To enable free trial mode, click the edit menu option **Free Trial (Disabled)**.



3. In the status bar is shown that the free trial mode is enabled and how many days are left.



Computers Hosting Application:

Host Name	IP Address
WIN-DPB5EQTD5E7	172.17.28.30

Free Instance Licenses: 0 of 1

Licenses Expire: never

Equipment Licenses:

Equipment Model	Used	Free
Employee	2	1998
Agent	0	500
Phone Based Agent	0	500
Supervisor	0	16
Operator	0	500
Voicemail Only User	0	2000
Additional Language	0	17
Soft Wallboard	0	64
VMP Port	4	196
VMP Port, Upgrade from HMP	0	0
Essential Employee	0	2000
CRM Integration	0	500
UC Connector (Skype for Business Integration)	0	500
Employee-Outlook Cal Intr. (on/off)	on	
Employee-VM to Email Intr. (on/off)	on	
Supervisor Full Reporting (on/off)	on	
Wallboard (on/off)	on	
Auto Attendant / IVR (on/off)	on	
Agent - Skillbased Routing (on/off)	on	
Identification Routing (on/off)	on	
Agent - Email Routing (on/off)	on	

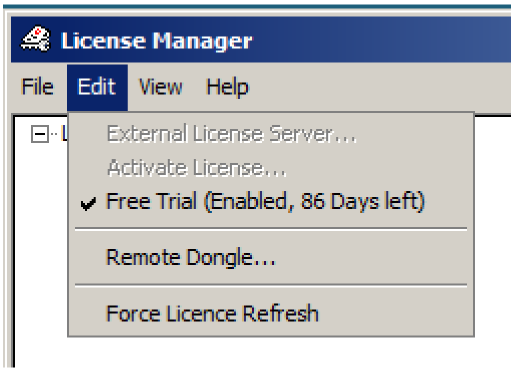
Functionality Licenses:

Agent - Outbound
Programming Interface
Web Callback
Call Recording
Web Chat
External Presence Integration
Post Call Survey
Social Media
Version 12.x

Ready

Free Trial (Enabled, 80 Days left)

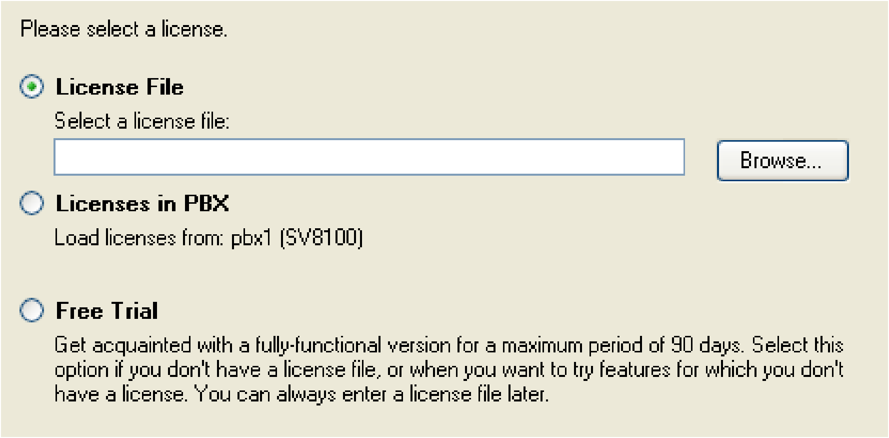
4. In the edit menu the free trial mode enabled is shown.



5. To disable / turn off the free trial mode, click the edit menu option “Free Trial (Enabled)”

Steps to activate in the BCT Configuration wizard

6. To start BCT in Free Trial mode select the Free Trial option in the license page in the wizard.



Please select a license.

◉ **License File**

Select a license file:

Browse...

○ **Licenses in PBX**

Load licenses from: pbx1 (SV8100)

○ **Free Trial**

Get acquainted with a fully-functional version for a maximum period of 90 days. Select this option if you don't have a license file, or when you want to try features for which you don't have a license. You can always enter a license file later.

7. To disable the free trial mode and / or load a license later, the license manager must be used.

1.5.2. Multiple BCT servers sharing a single license file

Preconditions

1. Use LMC as external license server.
2. LMC client must be version 5.2.0 or higher

What does it mean sharing a single license file for multiple BCT servers?

- One can have a single LMC license file that can be shared accross multiple BCT servers.
  The LMC license file has a number of BCT application licenses that is equal to the number of BCT servers that share the license file. This file must be loaded on a LMC client and all BCT servers must be configured to connect to this LMC client. This can be configured in the license manager by selecting the same LMC external license server (see 8.1.3.2 External License Server and 8.1.3.2.3 Use LMC to manage licenses)
- Every BCT server will claim a BCT application license and all related feature licenses are shared by the BCT servers and can be claimed until no licenses are available anymore. E.g. when 100 Agent licenses are present in the LMC license file, all BCT servers can claim Agent licenses until a total of 100 licenses are claimed. There are dynamic licenses like Agent, Operator and Supervisor and there are static licenses like Employee. Dynamic licenses are claimed and released when users sign in or out. Static licenses are set by configuration and will under normal condition hardly change. Functional feature licenses are only checked for presence in the license file. This means e.a. buying a license for Call Survey that it is valid for all BCT servers that share the license file.
- Every BCT server will only claim as many VMP licenses as VMP lines are configured on the system. When more VMP lines are configured then there are licenses available then only the number of available licenses are claimed. This means that one can configure more VMP lines then the available number of VMP licenses. In this case the number of operational VMP lines will be the number of claimed licenses and not the number of configured licenses. An Alarm is given about the mismatch (see 11.4.3.34 VMP (media port) License Alarm [6303]).
  When too many VMP lines were configured and the number of configured VMP lines becomes equal again to the number of claimed licenses, the alarm previously set will be cleared.
- In the system health tab of system settings (in case of shared license file), the license analysis rows will show the following license information: Used x, available y of z.

Note: For UNIVERGE 3C and multiple BCT servers, see also: *8.1.3.2.1 PBX-based License*

2. SYSTEM REQUIREMENTS

For Operating Systems requirements, see BCT Boundary Specification.

2.1. BCT Server requirements

Supported servers: all servers that fulfill the Hardware Compatibility List (HCL) of Microsoft and have the minimum requirements as stated in the BCT Boundary Specification.

2.2. SQL Server requirements

BCT uses an SQL database (by default called "United") to store data. You must decide which SQL Server version to use. In most cases, Microsoft SQL Server 2016 Express Edition, as available on the BCT product DVD, is sufficient. For other reasons (e.g. company maintenance or expected database size) you might want to use a SQL Server Standard or Enterprise Edition instead. The database server can be installed on the BCT server, or a dedicated remote database server.

For supported SQL server versions and requirements, see BCT Boundary Specification.

Note: *When using remote SQL server, the time difference between the BCT Server and the SQL server must be less than a few seconds. Use Microsoft Timeserver to synchronize times.*

Note: *During the installation the system administrator username (sa) and password are used, therefore the SQL Server authentication must be in mixed mode (SQL Server and Windows authentication).*

In case of a high load system, consider to use quad-core CPUs. Put the SQL server on 1 CPU and make sure that this CPU is not used by BCT runtime modules (UCS runtime, office server).

2.3. Client PC requirements

Supported client PCs: all client machines that fulfill the Hardware Compatibility List (HCL) of Microsoft and have the minimum requirements as stated in the BCT Boundary Specification.

On the client computer Microsoft Internet Explorer or Edge must be used as web browser during ClickOnce installation of BCT clients (see 9.1.1 Desktop Client). Otherwise another browser can be used as well.

2.4. Network information

In general UDP is used for communication in the BCT client/server communication. TCP-IP is used for communication that requires high reliability, such as between the BCT server and the database or the BCT Supervisor Dashboard clients.

2.4.1. Port usage

BCT Server ports		Client and / or Service ports		Comments
UDP	TCP	UDP	TCP	
BCT Server ⇔ Web-client (generic) (BCT-client / XML-terminal)				
	80		-	HTTP
	-		82	HTTP (push server port on XML terminals)
BCT Server ⇔ Open Web Interface (OWI) Clients				

BCT Server ports		Client and / or Service ports		Comments
UDP	TCP	UDP	TCP	
	32011		-	NEC FrontEnd Service (using SSL) Used by .NET clients when using Windows or cookie authentication and used by web javascript clients when using cookie authentication
	32013			NEC FrontEnd Service (using SSL) Used by web javascript clients when using Windows authentication
BCT Server ⇔ Social Media Providers				
	80/443			NEC Social Media Proxy, port 443 for secure connection
BCT Server ⇔ Database Server				
	-		1433	On the server where SQL Server is running with the default instance. When you have a named instance by default the listen port used is defined dynamically. It is recommended for a named instance to configure the database engine to listen on a specific port known as a fixed port or static port. For details see chapter 8.1.2.1 Windows Firewall configuration - Remote SQL Server access
BCT Server ⇔ Email Server (only if email routing exists)				
	-		25	SMTP Service
	-		465	SMTP Service using SSL
	-		587	SMTP Service using StartTLS
	-		110	POP3 Service
			995	POP3 Service using SSL
			143	IMAP Service
	-		993	IMAP Service using SSL
	-		443	Microsoft Graph Service (via standard HTTPS port)
BCT Server ⇔ BCT Clients (PC and smart phone)				
51870		51872 51873 etc		UCS Post Office Service (UDP communication) Clients are starting from port 51782. When more clients are started on the same PC, the port number is increased.
51871		51871		Broadcast / Multicast port (client listens only)
	1433		-	Applicable when on the BCT server a SQL Server is running with the default instance.
	5000		-	NEC CTI Service Used by 3rd party CTI platform application
	-		port	Hardware Wallboard (IP-based). Note that ‘port’ represents the configured service-port on the wallboard itself where BCT-Server will connect to.
	8745		-	NEC FrontEnd Service Used by BCT Supervisor Dashboard client and Directory Browser. Bound to this port is ‘BCT Connection Certificate’, a self-signed certificate created by BCT server installation for ensuring message security.
	8086		-	NEC Remoting Service Used by Desktop Client
	8087		-	NEC Remoting Service Used by Desktop Client (secure TCP port)
	9031		-	NEC Reporting Service Used by BCT Supervisor Dashboard client
	80		-	Used by Desktop Client (full directory access)
	32010		-	NEC FrontEnd Service (OWI internal) Used by Soft Wallboard client (only for BCT systems upgraded from before 9.x)
	32011		-	NEC FrontEnd Service (OWI internal) Used by BCT Agent smart phone app and Soft Wallboard client (using SSL)
BCT Server ⇔ Licensing (PBX, Supervisor, Remote Dongle)				
	-		6080	License port on SV8100/SV9100

BCT Server ports		Client and / or Service ports		Comments
UDP	TCP	UDP	TCP	
51670		-		License Manager verification for remote BCT Supervisor Dashboards
-		6001		Remote Dongle
BCT Server VMP (media ports) ⇔ PBX / Terminal Clients				
0		5060	5060	SIP signaling – Only with iS3000/SIP@Net and UNIVERGE 3C The VMP port default value is 0, but can be changed.
0		5070	5070	SIP signaling – Only with AspireX and SV8100/SV9100 The VMP port default value is 0, but can be changed.
0		5061	5061	Secured SIP Signalling (TLS) – Only supported with UNIVERGE 3C and SIP@Net
3456		3456		IP Protims signaling – Only with SV8300/SV9300 and SV8500/SV9500
49000 +1600 (range)		-		Media stream port range as used by VMP (for all platforms) Value 49000 is default, but can be changed. There are +1600 ports reserved: Max. 200 VMP lines, max 2 calls each with its own RTP+RTCP makes 800. This is doubled to prevent direct re-use of ports. The ports are increased per call and reset to the base-port when at +1600. This is independent of the VMP Port Licenses.
	8738		-	[Internally only] VMP Service WCF port (currently used internally only)
28000		28002		[Internally only] SIP-PDS Proxy and PDS Service communication channel
28000		28000-28017 + 28018 +3 ports per line		PDS Service towards PBX (Terminal signaling - NECDRS / PROTIMS / VoiceControl) Each line requires 3 ports, starting from 28018. So 16 VMP lines requires range: 28018 - 28065
BCT Server ⇔ PBX (CTI)				
	-		60030	CTI port for AspireX/AspireUX, SV8100/SV9100, SV8300/SV9300 and SV8500/SV9500
	-		8181	CTI port for SV9100-TAPI
	-		2555	CTI port for iS3000 / SIP@Net
	-		8088	HTTP (UNIVERGE 3C CTI port)
	-		443	HTTPS (secured UNIVERGE 3C CTI port using SSL)
BCT Server ⇔ PBX (MAT)				
	-		60000	MAT port for SV8300/SV9300 and SV8500/SV9500
	-		8010	MAT port for AspireX/AspireUX and SV8100/SV9100
	-		2596	OM port for iS3000 / SIP@Net
BCT Server ⇔ IP DECT Server (for Messaging and Central Directory)				
	-		2010	DAP Controller (DMLS)
	30160		-	DECT Manager (for Central Directory)

Note: *A client usually initiates the connection to the server (service) with a port assigned dynamically by OS.This is represented in above table as '-' or '0'.*

'0' means that the port is by default dynamically assigned, but is also configurable within BCT Tools. (e.g. the VMP SIP port). Most other BCT ports are also configurable, but this requires manual adaptation of certain configuration files and should be avoided (unless explicit documented in the manuals).

Note: *UNIVERGE 3C uses even port numbers for HTTP traffic, odd numbers are used for HTTPS traffic.*

Note: *An UDP heartbeat mechanism is running between client and server. This heartbeat is sent once every minute (unless other communication took place). This is a fixed interval, and cannot be changed.*

Between the server and the PBX, NO NAT router is allowed. So:

```
Client ──────────────────── Server ───────────────── PBX = OK

Client ──── FIREWALL ──── Server ───────────────── PBX = OK (if firewall is well configured)

Client ───── | NAT | ──── Server ───────────────── PBX = OK

Client ───── | NAT | ──── Server ──── |NAT| ────── PBX = Not OK!!

Client ───── | NAT | ──── Server ──── FIREWALL ─── PBX = OK (if firewall is well configured)
```

The server requires a fixed IP address, after network changes you must always restart the server, as the BCT communication layer continues with old settings until a reboot is done.

2.4.2. Broadcast / Multicast

By default, BCT uses Unicast communication.

For larger BCT systems (as an indication: above 100 agents / 750 employees) it is advised to use Broadcast (if allowed and possible) or Multicast communication to improve communication performance.

To switch to broadcasting or multicasting, use the Runtime Manager:

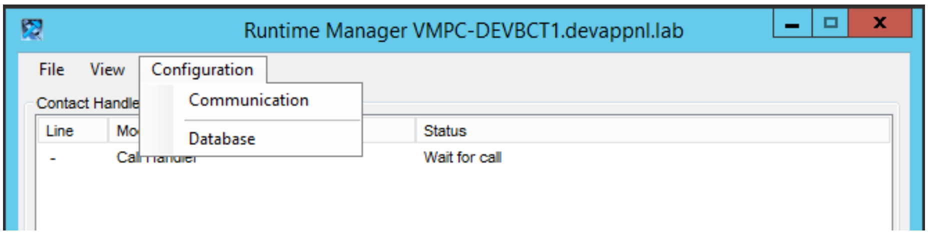
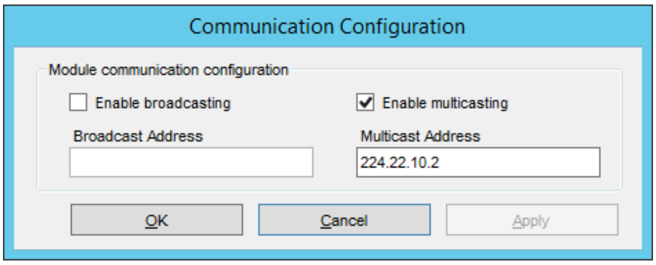


Figure 2-1 Runtime Manager - Main window

1. Select "Communication". The configuration window pops up.



Communication Configuration

Module communication configuration

☐ Enable broadcasting

☑ Enable multicasting

Broadcast Address

Multicast Address: 224.22.10.2

Figure 2-2 Runtime Manager - Communication Configuration window

2. Select either:

- **Enable broadcasting** and enter a broadcast address (depends on the subnet the BCT server and clients are part of or

- **Enable multicasting** and enter a multicast address (in the range 224.0.0.0 until 239.255.255.255)

Only one of both addresses can be enabled at a time.

***Note**: When either Enable broadcasting or Enable multicasting is set, the runtime should be stopped and restarted.*

2.5. IVR versus IVR-less Contact Centers

BCT supports both IVR and IVR-less Contact Center functionality. The choice depends on the wishes of the customer.

In an IVR configuration voice messages like welcome prompts can be played by VMP Software. VMP Software performs media processing tasks on the BCT server without requiring the use of specialized hardware.

An IVR less configuration lacks IVR prompts or announcements.

***Note**: In an IVR less configuration some messages can be provided by the PBX. For example, those supplied by the PN-4DAT board in the InMail board of the SV8100/SV9100. These PBX-generated messages can only be used for a general welcome message and 2 separate UCD delay announcement messages; they can't be used for Call Flow information (such as attendant or confirmation prompts.). These PBX generated messages can only be used for external parties calling in, not for internal calls.*

In an IVR less configuration a number of BCT Call Flow modules cannot be used. The following list gives an idea what kind of functionality is affected when IVR prompts are not available:

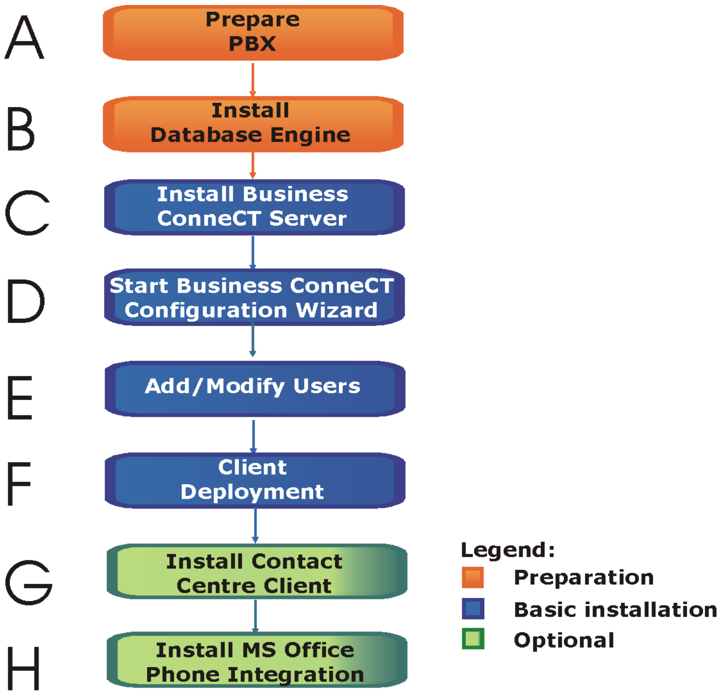
Starter module	In an IVR less configuration you still need a Starter Line to enter the Call Flow but no day period greetings or welcome greeting can be played during the starter period.
Attendant and option menu	Attendant and option menus cannot be used; the caller cannot be informed about the available options.
Message box	The message box requires prompting to inform agents or other users of the message box about choices that must be made
Identification module	Only the CLI and Called Number can be used. PID identification requires prompt guidance and input from the caller.
Phone based agent login via starter line	Agents can't be guided via prompting during the login session. This function is replaced by the “Server Dialed” prefixes or dedicated function keys on the agent's feature phone.
Call flow information prompting	In a lot of Call Flow modules you can inform callers that the phone call is sent to another module. E.g. “You will be transferred to the

operator”, “outside office hours” etc. This kind of prompting is not available in a system without IVR.

3. STEP PLAN SETTING UP BCT

To install BCT using the basic installation method, we assume that all requirements are met, the *stand-alone* PBX is prepared and a database is installed.

Installation flow chart:


A
Prepare PBX
B
Install Database Engine
C
Install Business ConneCT Server
D
Start Business ConneCT Configuration Wizard
E
Add/Modify Users
F
Client Deployment
G
Install Contact Centre Client
H
Install MS Office Phone Integration
Legend:
Preparation
Basic installation
Optional

For detailed information please refer to the relevant sections:

A 4.1 General
4.2 UNIVERGE SV8300/SV9300 configuration
4.3 UNIVERGE SV8500/SV9500 configuration
4.4 UNIVERGE SV8100/SV9100/AspireX/AspireUX configuration
0
iS3000 / SIP@Net configuration
4.6 BCT on UNIVERGE 3C

B 6 SERVER PREREQUISITES INSTALLATION

C 7 BCT SERVER PRODUCT INSTALLATION

D 8.1.1 Using the Configuration Wizard

> ***Note:*** *The terminal types are automatically retrieved by the PBX Synchronization. In case you need to set them manually – see 8.5.1.1 Set terminal type.*

E 8.5.6 Importing users

F 9 CLIENT INSTALLATION AND CONFIGURATION.

> ***Note****: The BCT Mobile Client Application is an integrated part of the BCT server platform. It is automatically installed. For configuration aspects of the BCT Mobile Client, see 8.1.13 BCT Mobile Client application and 9.5 Mobile Client.*

G 9.3 Contact Center (Supervisor) Client - PC

H 9.2 Client Integration – PC

4. PBX CONFIGURATION

4.1. General

4.1.1. Using VMP lines for IVR

BCT uses VMP software for Interactive Voice Response. VMP is running on the server and the VMP lines will act as IP terminals connected to the PBX. Therefore the codec settings for RTP packet exchange between BCT server and media end points needs to be configured in such a way that it is compatible with the codec abilities of VMP. A VMP line can handle codec G.711 a-law, µ-law and G.729. The payload is automatically configured. Although technically possible, we do not recommend codec G.729, as speech quality is much lower.

4.1.1.1. In-band DTMF detection

While VMP expects to receive out-of-band DTMF (RFC-2833 / Protims DTMF), recently also in-band DTMF has been introduced to cover some rare scenarios. The use of in-band DTMF detection is discouraged, since it is unreliable as it is part of the voice-media stream.

- For SIP-based IVR-lines (PBX's: 3C, SIP@Net and SV8100/SV9100) the in-band DTMF detection is attached automatically when no out-of-band DMTF (RFC-2833) is negotiated.
- For SV8300/SV9300 / SV8500/SV9500 in-band DTMF detection is by default disabled.
  In the case that it is required to enforce in-band DTMF anytime, a configuration flag has been introduced. You can find and change this configuration file by:
- Open the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common Files\NEC\VMP\VMPService.WinService.exe.config".
- Locate the key: enforceInBandDtmfDetection
- Set the value to: true
- Press Save to store the value.
- Restart the VMP service.
- Example scenario which would need above enforcement
  A SIP-terminal on SV8500/SV9500 that makes a call over CCIS towards a SV8300/SV9300 and arrives on a BCT IVR-line and needs DTMF action. Here at the receiving SV8300/SV9300 the enforcement is required to enable DTMF detection from the SIP-terminal.

4.1.1.2. Fine-tuning 'cut-off' of recordings – to prevent incomplete recordings (SIP only)

When a recording is stopped by means of DTMF-digit, and an analog- or ISDN trunk/terminal was used, then this DTMF can be heard at the end of the recording.
Because of this, the recording is truncated by cutting-off something at the end of the recording.
In certain situations it is possible that too much is cut-off, causing the end of the recording being incomplete. When required, the amount being cut-off can be fine-tuned with next configurable item:

```
<appSettings>
  <!-- Specify (in milli-seconds) the cut-off at end of recorded WAV-file.
       When a recording is stopped via DTMF, this cutting is applied to
       prevent inclusion of DTMF tones in the recording.
       Use 0 to disable, 2000 is maximum (default:750).               -->
  <add key="DtmfCutOff" value="750"/>
</appSettings>
```

4.1.1.3. Alarming on occupancy of VMP lines

To signal too much occupancy of the VMP lines with an alarm in the health page of System Settings:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config“.
2. Locate the keys: VmpOccupancyUpperThreshold and VmpOccupancyLowerThreshold
3. Set the values to: e.g. 80 resp. 60
   When the number of busy VMP lines increases and reaches the upper threshold (e.g. 80%) alarm 86030001 will be raised.
   When the number of busy VMP lines decreases and passes the lower threshold (e.g. 60%) the alarm will be cleared again.
4. Press Save to store the value.

4.1.2. Supported telephone sets and headsets

Office users can use all PBX-supported telephone sets and headsets, analogue, digital, IP or IP DECT. The use of analogue and IP DECT is restricted. However, users can’t answer or disconnect calls via the user interface of BCT. For analogue sets users also can’t put calls on hold with the UI.

Operators and Contact Center agents require a feature phone for the Fallback scenario. If the system fails they require sublines to handle the traffic.

***Note** (applicable for SV8300/SV9300 / SV8500/SV9500)**:** When connecting a headset to a DT-serie terminal for the first time, you must activate the headset mode by pressing a headset key while the extension is ringing and let the other party end the call first. You only need to do this the first time you connect the headset.*

***Note** (applicable for SV8100/SV9100 / AspireX/AspireUX): Program a headset Function Key (default function "05-Headset" in Function Key command 15-07). Go off hook and activate headset mode by dialing the Service Code number (for SV8100/SV9100 default 798, for AspireX/ApireUX program with command 11-11-65). After activating Headset mode, press the function key to go onhook. The Headset mode is now active.*

***Note** (applicable for UNIVERGE 3C): Agents can use Polycom models 320, 330, 430, 501, 550 or the 650. Employees can use all Polycom sets as supported for agents including headsets. Employees can also use IP-DECT handsets.*

4.1.3. Router information of Contact Center call on feature phones

BCT shows router information on the display of feature phone of agents when receiving Contact Center calls. The router information that is shows depend on the PBX type and the terminals type:

- On SV8300 the called number, the calling party and the Router name is shown on the display of DT300 and DT700 terminals.
- On SV9300 the called number, the calling party and the Router name is shown on the display of DT400, DT500, DT800 and DT900 terminals.
- On SV8500 the called number is shown on the display of DT300 and DT700 terminals.
- On SV9500 the called number is shown on the display of DT400, DT500, DT800 and DT900 terminals.

- On iS3000 the calling number is shown on the display Ergoline and Sophoset terminals.

To suppress this information see 11.3.14 Agent Display Information overwritten.

4.1.4. Silent monitoring

Within SV8300/SV9300, SV9500, SV8100/SV9100, Univerge 3C, SIP@Net (server only) and AspireX/AspireUX it is possible to monitor a conversation without giving any indication to the parties in conversation. This function is often used during coaching of contact center agents. In order to avoid interaction with the intrude (break-in/barge) function of operators it is strongly advised to activate this function for a Class of Service only containing supervisors of contact center agents.

By default, the supervised party sees a notification of being monitored or barged. For monitoring this may be experienced as undesired.

To suppress monitored notification:

1. Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example. Default location: C:\Program Files (x86)\NEC\UCS-Module\Server.

2. Enable / Include:

   ```
   <add key="SuppressMonitoredStatus" value="True"/>
   ```

   (Note that the key might be present in a comment block, so include it outside the comment)

3. Save the file.

***Note:** Monitoring telephone conversations **may be illegal** under certain circumstances and laws. Consult a legal advisor before implementing the monitoring of telephone conversations. Some federal and state laws require a party monitoring a telephone conversation to use beep-tones, to notify all parties to the telephone conversation, and/or obtain consent from all parties to the telephone conversation. Some of these laws provide strict penalties for illegal monitoring of telephone conversations.*

4.1.5. Routing Points

Routing Points are generally applied in various PBX-types (see below). Routing Points can be used internally in BCT call processing of specific scenarios. Therefore it is advised to configure at least one Routing Point.

4.1.6. Restart of UCS Runtime

After a change in the PBX configuration (including changes in AD for PBX-type UNIVERGE 3C), synchronization and a restart of the UCS Runtime is required when:

- Phone Based Agent role has been changed or
- Properties of an extension have been changed via System Settings (e.g. override Terminal-type, area etc.)

4.1.7. Call Recording

4.1.7.1. User-initiated Call Recording

To allow user initiated call recording, it could be that depending on PBX type some settings must be set, e.g. 4.5.12 Call Recording

4.1.7.2. PBX Configuration for SIP@Net Call Recording

See 4.5.12 Call Recording

4.1.7.3. dvsAnalytics Encore configuration for dvsAnalytics Encore recording

No additional configuration settings is required other than the standard configuration requirements for the dvsAnalytics Encore 3rd party product.

4.1.7.4. "BCT Compliance Recording" configuration for "BCT Compliance Recording"

No additional configuration settings is required other than the configuration requirements for the "BCT Compliance Recording" product.

4.2. UNIVERGE SV8300/SV9300 configuration

This chapter explains how to set up the PBX types SV8300/SV9300 for BCT. The main configuration items concern voicemail, operators and Contact Center.

For the **voicemail** functionality, calls are queued on VMP lines.

For the **operator** the configuration is without IVR. In this case the calls are queued in the PBX. The callers are queued on Routing Points until an available operator is found. In this case, the maximum number of callers that can be queued is not restricted by the number of available VMP lines. A configuration application that uses Routing Points without IVR for queuing is called an IVR less configuration.

For the **Contact Center** functionality, both IVR configuration and IVR less configuration are supported. The choice depends on the requirements of the customer, for more information, see 2.5 IVR versus IVR-less Contact Centers.

Please refer to the Release Notes to check the PBX compatibility.

You program the SV8300/SV9300 with PC Pro.

4.2.1. SV8300 and SV9300 differences

If you are using a SV9300 instead of a SV8300, be aware that in SV9300 the meaning of data for some commands are changed, see chapter "System data improvements for SV9300" in the command manual of the SV9300. For BCT configuration only the follwing data that is change:

- For SV8300 **08 > 379 > 0;** Activate name display / calling party number display notification for calls terminating from a CCIS terminal.
- For SV9300 **08 > 379 > 1;** Activate name display / calling party number display notification for calls terminating from a CCIS terminal.

4.2.2. Scripts and examples

You can use the scripts on the BCT product DVD (PBX Scripts folder) as a basis for projecting a standalone PBX system. The scripts contain a standard operator, voicemail, and starter entries. In this manual, the projecting of the PBX follows the examples of the figures in the following sections. The examples can be used after a System Data/SRAM clear on the PBX and configure the PBX with a 2xx digit number plan.

You must change the station numbers, hardware addresses etc. to the ones you require.

4.2.3. Configuration overview

BCT contains four major parts that all are connected to the PBX:

Employee

The Employees are based on individual station numbers. To monitor and control the stations BCT uses the OAI link.

Operator

The operator is based on an IVR less configuration of the PBX. This means the operator uses a group of Virtual extensions programmed as Routing Points for the calls to the operator. An example is given in Figure 4-1 Example of operator routing points and fallback numbers.

A Routing Point in a SV8300/SV9300 is a Virtual extension, setup as an (OAI) Monitored number. A Monitored number means that calls to this number and call related information are sent over the OAI interface to an external application. This external application is BCT that recognize this (OAI) Monitored number as Routing Point. When the external application is down, the PBX notices this and the Monitored number acts as a normal UCD pilot number in a group, thus allowing an automated Fallback scenario.

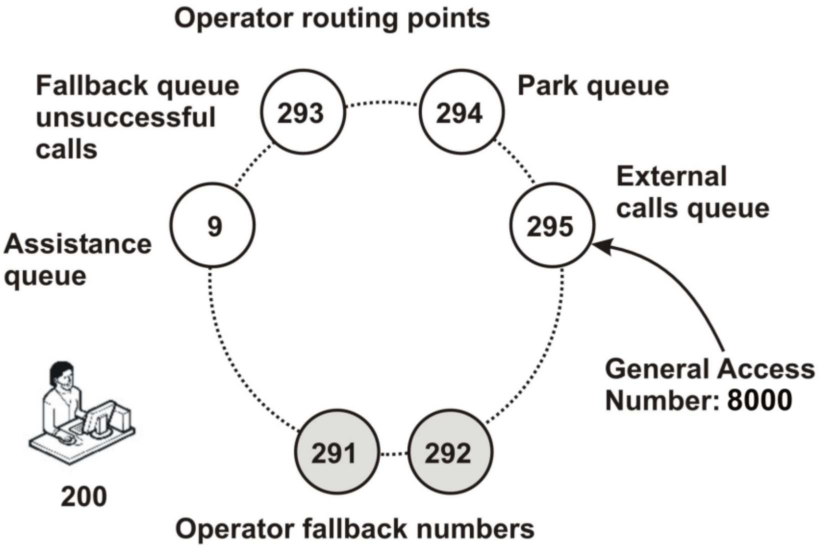


Figure 4-1 Example of operator routing points and fallback numbers

For the operator, more than one Routing Point is required (assistance, external incoming calls, fallback of unsuccessful calls and park). Using the Configuration Wizard (or the BCT Supervisor Dashboard application), the Routing Points are connected to Starter Lines. In this way the operator can see what kind of call it is.

In IVR less configurations, features like music on hold, prompts and Queue announcements cannot be played. For the Operator, a combination with IVR is allowed. In that case the routing takes place via the IVR less configurations and IVR features are available as well. Each time an IVR feature is required the call occupies an VMP line.

All Routing Points are combined in a group together with fall back sub line numbers. These sub line numbers are programmed on the DT-phone of the operator. The Fallback scenario for IVR less configurations is automated, meaning no user input is required when the OAI connection fails.

Voicemail

The voicemail application uses an IVR configuration to play announcements and receive user input. In an IVR configuration the VMP lines are configured in the PBX and are connected to the VMP software of BCT that will handle the calls on the VMP lines.

In a SV8300/SV9300 an VMP line is implemented by an IP Dterm extension that is configured as an IP Dect terminal. This extension is registered by the VMP software of BCT. The VMP lines are configured in a group together with a virtual pilot number. To distinguish incoming voicemail calls from other call to the IVR group, you program an access number. This access number is a Virtual extension with call-forwarding to the virtual pilot of the IVR group so calls to the access number will end up at a free VMP line.

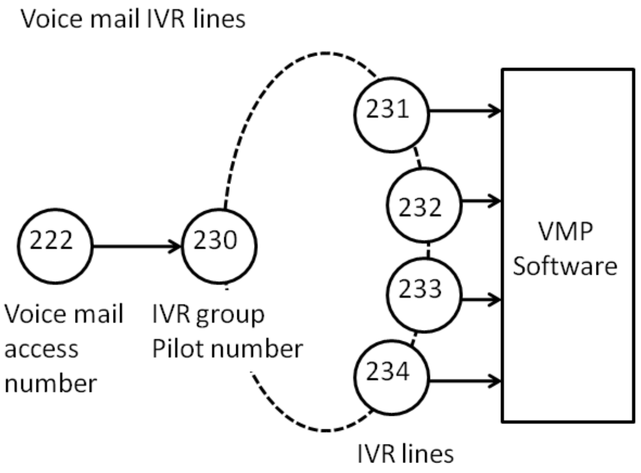


Figure 4-2 Voicemail access and IVR/VMP lines example

Contact Center

The Contact Center application supports both IVR less configurations and IVR configuration of the PBX.

As stated before, an IVR less configuration uses Virtual extensions programmed as (OAI) Monitored number. BCT recognize this (OAI) Monitored number as Routing Point that can be used for the calls to the Contact Center. These Routing Points are monitored by the BCT server via the OAI link. Queuing of calls is done on these Routing Points. An example is given in Figure 4-3 IVR-less Contact Center example. Also for the IVR-less Contact Center configuration, a combination with IVR is allowed. In that case the routing takes place via the IVR less configurations and IVR features are available as well. Each time an IVR feature is required the call occupies an VMP line.

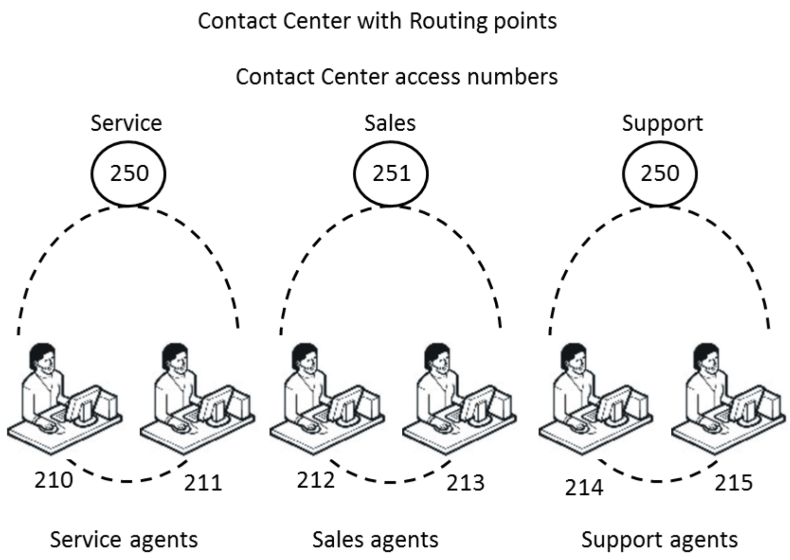


Figure 4-3 IVR-less Contact Center example

All Routing Points are combined in a group together with fall back numbers. These numbers are either the extensions of the agents themselves or fallback sublines numbers programmed on the DT-serie terminals of the Contact Center agent. The Fallback scenario for IVR less configurations is automated, meaning no user input is required when the OAI connection fails.

An IVR configuration uses VMP lines as Voice Media Ports (VMP) to play announcements and receive user input. In a SV8300/SV9300 the VMP line is implemented by an IP Dterm extension that is configured as an IP Dect terminal. This extension is registered by the VMP software of BCT.

The VMP lines are added to a group together with a virtual pilot number. Access numbers can be programmed to distinguish different services and play the appropriate announcement. The example Figure 4-4 Contact Center with IVR/VMP lines example uses three access numbers. All calls to these access numbers are forwarded to the pilot number of the IVR group.

The Fallback scenario for an IVR configuration has to be handled manually. The access numbers have to be manually forwarded to a group of agent extensions who provide the required service.

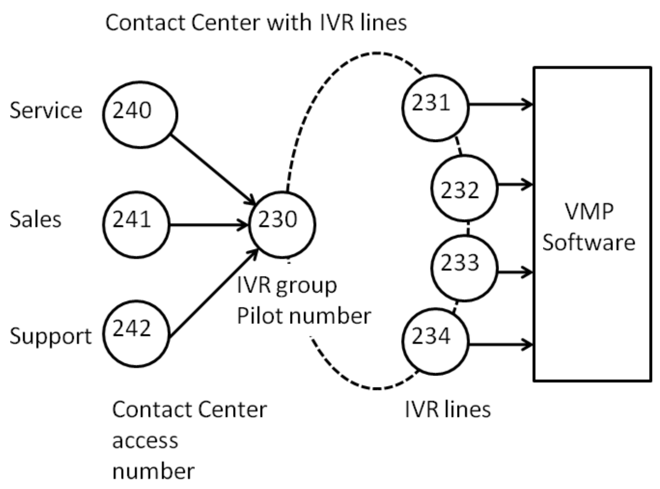


Figure 4-4 Contact Center with IVR/VMP lines example

4.2.4. Boundaries, options and timers

The system only works when you use the correct values for the PBX boundaries, options and timers for BCT.

Boundaries

- UCD/ACD group numbers: a maximum of 16 in a single PBX.
- UCD/ACD group members: a maximum of 60 per single group.

Options

These options have to do with sending the Status Monitor Facility Notification (SMFN) via the OAI link to the BCT server, and to make sure the system behaves correctly during hold/transfer call situations.

08 > 028 > 0; Allows BLIND TRANSFER on trunk.

08 > 117 > 0; When talking to party-B, with trunk-A on hold, return to trunk-A after party-B hangs up.

08 > 124 > 0; Activate multiple connections on announcement service.

08 > 177 > 0; Activate LAST NUMBER CALL (Last Number Redial). This command ensures that if a caller is transferred unsuccessfully the call will fall back to the originally called party, essential for the operator.

08 > 212 > 1; When a caller encounters all ACD/UCD stations busy, caller is placed in queuing mode.

08 > 254 > 1; Function of hold key is Hold.

08 > 379 > 0; Activate name display / calling party number display notification for calls terminating from a CCIS terminal.

Note: difference between SV8300/SV9300 see SV8300 and SV9300 differences

08 > 460 > 0; Send OAI SMFN STS (status) for Call Transfer from station.

08 > 461 > 0; Send OAI SMFN when answering held call. Define phone type for OAI SMFN: single line telephone.

08 > 462 > 0; Send caller ID.

08 > 464 > 1; Activate (OFF)HOOK for SCF MakeCall.

08 > 465 > 0; Activate detailed error information.

08 > 534 > 0; When talking to trunk-B, with trunk-A on hold, return to trunk-A after trunk-B hangs up.

08 > 669 > 0; Activate Do Not Disturb notification across CCIS.

08 > 804 > 0; Define phone type for OAI SMFN: single line telephone.

08 > 805 > 0; OAI SMFN (Status) when the forwarded call with Call Forwarding-No Answer (Don't Answer) is terminated to a station.

08 > 808 > 0; Activate answer forward all/ forward busy/forward no answer events.

08 > 809 > 1; Activate exchange of line info when answering a hold connection with answer call.

08 > 811 > 0; Activate incoming forward all/ forward busy events.

08 > 815 > 0; Activate incoming recall when Exclusive hold calls recalls.

08 > 816 > 0; Enable 3rd party line and 3rd party info in SMFM1.0 and SMFM 2.0

08 > 817 > 0; Activate incoming and answer forward all/ forward busy/forward no answer events for calls via CCIS are ringing or answered.

08 > 818 > 0; Activate hold exclusive when a call is put on exclusive hold.

360> TRCIN+TRCOUT > 0; Allows TRANSFER on route.

08 > 839 > 0; Send OAI SMFN with intermediate information via OAI queue (ON)

08 > 840 > 0; Send OAI SMFN when setting CAMP ON

08 > 843 > 0; Enable shuttling back via OAI to released hold party

08 > 845 > 0; Automatically reconnect to hold party when active party released

08 > 846 > 0; Setting Camp On to destination when Call Forwarding-All is set

08 > 847 > 0; Send OAI SMFN when setting Camp On

6527 > tenant number > 1; Automatic Call Distribution OFF

6528 > tenant number > 1; RR sending priority when receiving OAI SCF

08 > 685 > 0; Send DTMF signals to the other office station/trunk when the connection between DT700/DT800/DT900 Series via IPT (P2P CCIS) and other office station/trunk is established.

These settings are necessary to send the correct events over the OAI link to BCT.

To use functionalities of BCT, the stations of users need to be able to use some features, like consultation hold and Conference. In a default configuration all stations are able to use these features. When your system has been modified then use the following commands to verify and correct the features.

To allow set/reset call forwarding (presents) from the station:

1202 > station > ClassA-ClassB;

15000 > Class A > 1; allows Call Forwarding All calls

To allow consultation hold:

1207 > station > Class C; Assign the station to a certain Service restriction calls C

15088> Class C > 1; Switch Hook Flash effective for internal calls

15089 > Class C > 1; Switch Hook Flash effective for internal calls

15090> Class C > 1; Switch Hook Flash effective for external calls

12091 > Class C > 1; Switch Hook Flash effective for external calls

Do not program trunk line keys on stations used by BCT.

To allow activation of call waiting:

1202 > station > ClassA-ClassB; Assign the station to a certain Service restriction class B
15044 > Class A > 1; allow Call Waiting answer – calling side

To answer a call waiting:

1202 > station > ClassA-ClassB; Assign the station to a certain Service restriction class B
15072> Class B > 0; allow stations in Class B to use the Answer key

To allow conference and call recording by BCT user:

08 > 101 > 1;	Enable 3 party conference among stations
08 > 102 > 1;	Activate conference with HookFlash when connected and have party on hold
08 > 103 > 1;	Enable 3 party conference among stations and trunk
08 > 104 > 1;	Activate conference with HookFlash when connected and have party on hold
456 > 00 > 1;	Set conference trunk in service
457 > 00 > 1;	Use conference trunk also for stations

To allow blind transfer:

08 > 062 > 1 Allow call transfer from station before called station answers

If DT700/DT800/DT900 terminals are used, mind the following point:

An DT700/DT800/DT900 user can login and logout the extension to prohibit the use of it by unauthorized users. For a logged in extension, the status indication in BCT is according to the status of the phone number: idle, ringing, busy, etc. For a logged out extension, the status indication in BCT is NOT according to the status of the extension. A logged out extension has the status indication 'idle', because there is no status indication defined for an unassigned number. A call to the logged out extension has the status indication 'ringing' and the caller hears ring tone, but there is no DT700/DT800/DT900 terminal ringing.

You can change the behavior of the unassigned number with CM 15481 > Station No. > 02. With this option the caller will hear busy tone instead of ringing and a call from BCT to this unassigned number is not possible.

Timers

You can change the No Answer time-out time by using the following command. This determines the time that an external party rings on an extension before enter the fallback Queue of the operator. The default is between 32 and 36 sec.

410 > 01 > .. Elapsed time for Call Forwarding No answer Trunk calls.

You can change the Camp On time-out timer by using the following command. This determines the time after which a call returns to the operator, in the case where the operator transfers a call to a busy station that remains busy. The default is 24 to 32 seconds.

410 > 26 > .. Automatic Recall Timing of Camp-On

License

BCT requires an OAI licenses in the PBX to connect to the PBX. Use following command to check if OAI licenses is available:

F87 > 005 : A	OAI licenses Avaialble.

4.2.5. Connection to a PBX

The CPU blade of the PBX is equipped with a VoIPDB card. This card is equipped with a standard RJ45 LAN connector; therefore it is possible to connect the PBX directly to the customer's LAN. For security reasons however, it is recommends to use a separate PBX LAN instead. This way the PBX is not accessible directly from the LAN. This can be a VLAN configuration. The next figure gives a schematic overview and the use of IP address information, of this minimal configuration.

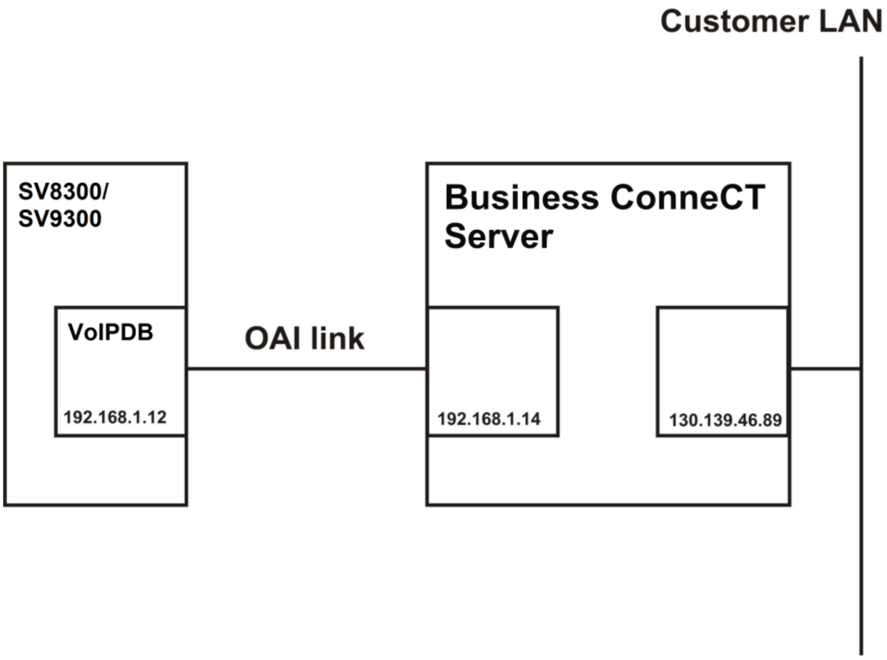


Figure 4-5 Minimal secure connection of a BCT Server

In this example IP address 192.168.1.12 is used for the PBX, this is a Class "C" IP address, so the Sub Net Mask will be 255.255.255.0

An example of checking/setting the IP address and sub net mask of the system:

0B101 > 00 > 192168001012;	IP address of the MP card.
0B101 > 01 > 255255255000;	Sub net mask of the MP card.
0B101 > 02 > 192168001254;	Default router IP address.

0B001 > 41 > 3; “3" means: OIA port number = 60030.

0B001 > 91 > 1; “1" means: Port selection for OAI is VOIP port.

Default router needs only to be defined, when necessary in the network. OAI port 60030 is fixed; the setting should always be '3' for the PBX. The IP address for the BCT server in this case can be selected from the same range as the IP address of the PBX. In the example above, the IP address 192.168.1.14 is used.

If a more advanced VLAN configuration is used the only consideration is the PBX and the BCT server must be able to see each other (ping). There is no need to use the same range of IP-addresses as long as it is configured correctly in the connecting router.

4.2.6. PBX projecting for the operator

Figure 4-1 Example of operator routing points and fallback numbers is used as example for this projecting. The numbers 9, 293, 294 and 295 in this example are used to create the operator Queues. When the OAI link is down for whatever reason the operator has to go into Fallback mode. In this example two sub line (291 and 292) numbers are programmed on the operator Dterm to handle calls.

4.2.6.1. Program Operator Routing Points

1. Define Virtual extension '9' as a one-digit number:

   200 > 9 > 801;

2. If using the example from this manual, define all operator Queues as three-digit numbers:
   200 > 2 > 803; all numbers starting with 2 will be three-digit.

3. Program virtual numbers:

11 > 500 > 9;	Create virtual Assistance Queue.
11 > 501 > 293;	Create virtual FallBack Queue.
11 > 502 > 294;	Create virtual Park Queue.
11 > 503 > 295;	Create virtual External Call Queue.
11 > 504 > 291;	Subline number for fall back if the server is down.
11 > 505 > 292;	Subline number for fall back if the server is down.

4. Define the virtual numbers as OAI monitored numbers:

   171 > 9 > 3;
   171 > 293 > 3;
   171 > 294 > 3;
   171 > 295 > 3;
   171 > 291 > 2;
   171 > 292 > 2.

5. Put all virtual numbers in a group, in this example UCD group number 15 is used:

   172 > 9 > 15;
   172 > 293 > 15;
   172 > 294 > 15;
   172 > 295 > 15;
   172 > 291 > 15;
   172 > 292 > 15.

6. Make all OAI monitored numbers busy, they are queued by the system, not on the PBX:

   E50 > 9 > 0;
   E50 > 293 > 0;
   E50 > 294 > 0;
   E50 > 295 > 0.

7. Define the group call direction, if the operator is called during fall back the calls go to 291 and 292:

   170 > 9 > 291;
   170 > 291 > 292;
   170 > 292 > 293;
   170 > 293 > 294;
   170 > 294 > 295;
   170 > 295 > 9;

8. The operator fallback (unsuccessful calls) Queue is not dialed by people but triggered by events in the system instead. These events must be programmed via the following automatic transfer commands:

   5100 > 01 > 293; DID destination on no answer time out to operator fallback Queue.
   5103 > 01 > 293; DID destination on busy time out to operator fallback Queue.
   5106 > 01 > 293; DID destination on unassigned nr. to operator fallback Queue.
   5110 > 01 > 293; Destination when called party has set DND to operator fallback Queue.
   5118 > 01 > 293; Transfer destination (to VMS) of the call that is set Camp-On and not answered/Transfer.
   5122 > 01 > 293; Destination when calling party is restricted for outgoing calls.

   Notes: *- Some of these events rely on system timers to be set.*
   - Redirecting some of these events to the operator might not be according to the customer's wishes.

9. In case Digit conversion is used in the PBX also the General Access number (and other numbers that need to be accessible from outside) need to be converted. In Figure 4.1 "Example of operator routing points and fallback numbers" the General Access number 8000 must be converted to station number 295 which is used for External Queue.

10. If for some reason the BCT server cannot be reached, the system will go to Fallback mode. In Fallback mode, the calls to the operator are routed to the Fallback subline numbers, in our example 291 and 292. To handle calls, these numbers must be programmed as sublines on the operator DT-serie terminal:

    9000 > 200,06 > 291;
    9000 > 200,07 > 292;

11. The operator terminal needs to be able to execute some features to fore fill its task, e.g. Break-in and Camp On. In a default system all stations are able to use these features. When your system has been modified use the following commands to verify and correct the values.

    To allow Break-in:

    1202 > 200 > ClassA-ClassB assign operator terminal to certain Service restriction class-A
    15005> Class-A > 1 Allow stations in Service restriction class to Executive Override
    456 > 00 > 1 Set conference trunk on MP-card in service

    To allow Camp on:

    08 > 146 > 0; Automatic Camp On available

08 > 147 > 0; Manual Camp On by use of access code

1202 > 200 > ClassA-ClassB; Assign operator terminal to certain Service restriction class-A

15016> Class-A > 1; Allow stations in Service restriction class to Camp On Transfer Mode

See also the Feature and Specification manual of the PBX.

4.2.6.2. Program Operator System Call Park Routing Points

To use the System Call Park functionality for operators (also called Pickup Park) a separate set of routing points need to be programmed. For every System Call Park position a routing point need to be created. In the example below three System Call Park positions are programmed:

1. Program virtual numbers:

   11 > 560 > 260;
   11 > 561 > 261;
   11 > 562 > 262;

2. Define the virtual numbers as OAI monitored numbers:

   171 > 260 > 3;
   171 > 261 > 3;
   171 > 262 > 3;

3. Put all virtual numbers in a group, in this example UCD group number 15 is used:

   172 > 260 > 15;
   172 > 261 > 15;
   172 > 262 > 15;

4. Make all OAI monitored numbers busy:

   E50 > 260 > 0;
   E50 > 261 > 0;
   E50 > 262 > 0;

   The numbers 260, 261 and 262 will now be seen as routing points by BCT and can be used for System Call Park. For BCT configuration for System Call Park see 8.3.10 Create System Call Park configuration.

4.2.6.3. BCT Operator in PBX networks (CCIS)

BCT can be used as central operator in a PBX Network. BCT only supports a closed numbering plan, so each number in the network should be unique. It should be possible to call all desired numbers from any PBX in the network, e.g. operator Queues, extensions of clients and trunk access codes. This means that numbers that do not reside in a local PBX should be routed over CCIS to the PBX where the number resides.

Although BCT physically accesses the PBXs as separate PBXs, logically the PBX network behaves as a single PBX, see Figure 4-1 Example of operator routing points and fallback numbers.

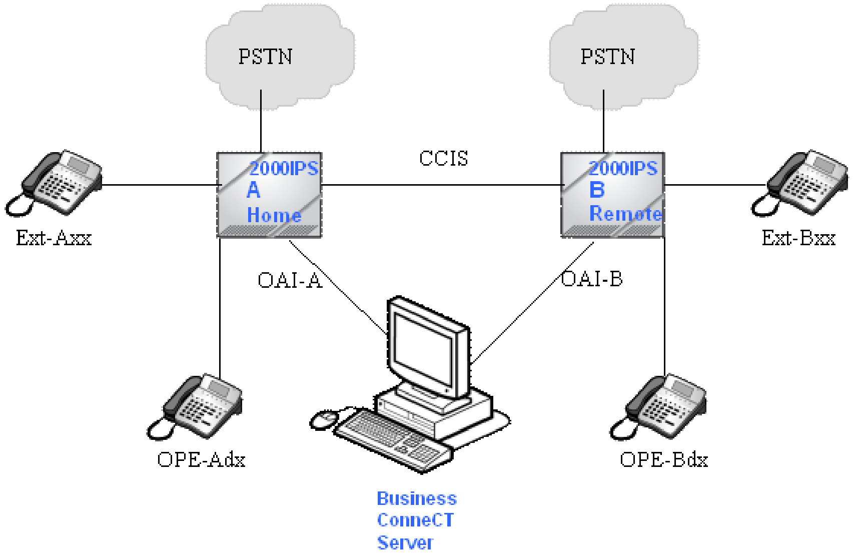


Figure 4-6 BCT in a multi PBX environment

Usually there is only a single internal number to call operator assistance. That means that the internal Queue resides in one PBX only (the Home PBX-A). The other PBXs (remote PBX-B) should be configured such that they route the internal Queue over CCIS to the Home PBX-A. In BCT Supervisor Dashboard there will be only one Starter Line for the internal Queue that is linked to the Operator Router, see section 8.3.3 Create Operator Starter and Starter lines.

In the example both the Home PBX-A and the Remote PBX-B have a trunk to the PSTN network. There are two ways to call the operator from the PSTN over both trunks:

- Calls from the PSTN network to the operator could go to a single external Queue in the Home PBX-A. The dialed number from the PSTN network connected to the Remote PBX-B should then be routed over CCIS to the external Queue in Home PBX-A. In BCT Supervisor Dashboard there will be only one Starter Line for this external Queue.

- Calls from the PSTN network to the operator go to a separate external Queue in each PBX. In each PBX an external Queue should be configured and in BCT every Queue should get its own Starter Line.

To park a call, each PBX should have its own park Queue. In BCT each park Queue should have its own Starter Line.

To handle unsuccessful calls each PBX should have its own Fallback Queue. In BCT each Fallback Queue should have its own Starter Line.

Table 4-1 Operator starter line configuration in CCIS networks shows an overview of the Queues and Starter Lines that need to be configured in the PBX CCIS network and in BCT.

Starter Lines	**PBX-A Home**	**PBX-B Remote**	**Router**
Internal	9	none	Operator
Fallback	293	193	Operator
Park	294	194	Operator

External	295	195 or none	Operator

Table 4-1 Operator starter line configuration in CCIS networks

In general, program both PBX systems as for 2 single BCT systems. The Routing Points of Figure 4-1 Example of operator routing points and fallback numbers are routed to the same group of operators by BCT. You create Starter Lines to the same Operator Router, see 8.3.3 Create Operator Starter and Starter lines.

1. Project DDI Fail in both PBXs: see 4.2.6.1 Program Operator Routing Points.

2. Project Automatic transfer on unassigned numbers for TEI in PBX-A.
   External calls dialing busy, no answer and DND extensions via CCIS should also be routed to the operator. Do not program Automatic transfer of failed TIE calls to the fallback Queue (5101, 5104 and 5107). TIE line fallback make that internal calls to busy extensions via CCIS are also routed to the operator, this give extra unwanted traffic. Also break-in over CCIS and camp-on busy over CCIS will not work with these Automatic transfer commands programmed. With Split Call forwarding it is possible to make a distinction between the internal calls and external calls via the TIE line. This is programmed in the following way:

   08 > 241 > 1;
   08 > 600 > 0;
   08 > 608 > 1;
   08 > 564 > 0; Should be programmed in both PBX-A and PBX-B.
   6523 > 01 > 1;
   6524 > 01 > 0;
   6525 > 01 > 1;
   78 > 010 > 293; Fallback number.
   CCH is CommonChannelHandle of CCIS route
   SV8300: A726 > CCH > 0, A728 > CCH > 0, A729 > CCH > 0;
   SV9300: A726 > CCH > 1, A728 > CCH > 1, A729 > CCH > 0;

   The following 2 commands should be executed for every extension.

   E604>Extension>8; Destination of call forwarding
   E605>Extension>0; Destination split forwarding Busy/No Answer

3. Project Automatic transfer on unassigned numbers for TEI: If PBX-B has PSTN as well PBX-B should be programmed too.

   08 > 241 > 1;
   08 > 600 > 0;
   08 > 608 > 1;
   08 > 564 > 0; Should be programmed in both PBX-A and PBX-B.
   6523 > 01 > 1;
   6524 > 01 > 0;
   6525 > 01 > 1;
   78 > 010 > 193; Fallback number.
   CCH is CommonChannelHandle of CCIS route

SV8300: A726 > CCH > 0, A728 > CCH > 0, A729 > CCH > 0;
SV9300: A726 > CCH > 1, A728 > CCH > 1, A729 > CCH > 0;

The following 2 commands should be executed for every extension:

E604>Extension>8;
E605>Extension>0;

4. Project access codes for split call forwarding:

   200 > accesscode > A182; Define number to set Split Call Forwarding All.
   200 > accesscode > A183; Define number to reset Split Call Forwarding All.

4.2.7. PBX configuration for Voicemail

4.2.7.1. Program VMP Lines

Figure 4-2 Voicemail access and IVR/VMP lines example shows a schematic overview of the IVR configuration. The callers dial the access numbers for Voicemail which are all forwarded to a Pilot number of the UCD group with the VMP lines as members. The VMP lines are IP Dterm extensions that are programmed as IP Dect extensions. These IP Dect extensions are configured as VMP lines and registered by the VMP software. All access numbers are set as Virtual extension.

Execute the following procedure to configure IP DTerm extensions as IP Dect extensions:

1. Enter the following commands:

   310 > 0 > NationCode ; NationCode specific assignment to EAM (e.g 04 for Asia/Africa/Europe/Latin America/Middle Ease/Russia, 03 for North America, etc)
   08 > 513 > 1; IPregistration method = per command 15>480
   08 > 514 > 1; Don't encode IP DECT DNR
   08 > 515 > 0; Don't encode IP DECT password

2. To configure a working IP DECT line , assuming all other settings are still default, use:

14 > free virtual LEN > F<Extension>;	Assign station number to LEN
93 > my line > Extension;	Assign prime line to station line
9000 > my line,key no. > Extension;	place the MyLine key at key 16
9000 > my line,01. > CCC;	Clear the MyLine key at key 1
9000 > **my line,key no. > LogOutKey;**	Define LogOut key (function key 15)
1202 > Extension > ClassA-ClassB ;	Set the extension in Service Restriction Class A (and Class B)
1207 > Extension > ClassC;	Set the extension in Service Restriction Class C
15143 > ClassA > 0;	Allow Logout for the Class A of the extension
15481 > ClassC > 03;	Allow Call Forwarding logout of the Class C of the extension

Example:
14 > 19000 > F231
93 > 231 > 231
9000 > 231,16 > 231
9000 > 231,01 > CCC

```
9000 > 231,15 > F0B39
1202 > 231 > 1415
1207 > 231 > 15
15143 > 14 > 0
15481 > 15 > 03
```

Execute the following procedure to configure the IP Dect extensions as VMP lines in the IVR group:

1. Put the IP Dect extensions used for VMP lines in a UCD group. Incoming calls are routed to VMP lines based on “longest idle".

   Example:

   ```
   11 > 506 > 230;   Group nr 230 is assigned as virtual pilot number.
   E50 > 230 > 0;    Group nr 230 set to BUSY.
   170 > 230 > 231; Create UCD group of IP Dect extensions and the virtual pilot number.
   170 > 231 > 232;
   170 > 232 > 233;
   170 > 233 > 234;
   170 > 234 > 230;
   171 > 230 > 1;    UCD pilot member definition.
   171 > 231 > 0;    UCD member definition. (Default setting)
   171 > 232 > 0;
   171 > 233 > 0;
   171 > 234 > 0;
   172 > 230 > 14;   Member assignment to UCD group 14.
   172 > 231 > 14;
   172 > 232 > 14;
   172 > 233 > 14;
   172 > 234 > 14;
   1324 > 231 > 1;   Digital Multiline terminal. (Default setting)
   1324 > 232 > 1;
   1324 > 233 > 1;
   1324 > 234 > 1;
   1359 > 231 > 1;   In-Skin UMS. (Default setting)
   1359 > 232 > 1;
   1359 > 233 > 1;
   1359 > 234 > 1;
   1368 > 231 > 0;   DTMP signal is transmitted from DT700/DT800/DT900 to Dterm IP.
   1368 > 232 > 0;
   1368 > 233 > 0;
   1368 > 234 > 0;
   ```

2. The voicemail application needs its own access number. Create a virtual number with ‘call forwarding all calls’ to the pilot number of the VMP lines. In our example this is the pilot number 230 of the UCD hunting group. The following example creates the access numbers from Figure 4-2 Voicemail access and IVR/VMP lines example.

Create the voicemail access number:

11 > 507 > 222; Assigns virtual number 222

Forward all voicemail access calls to the Routing Point:

E600 > 222 > 230; Call Forwarding all calls to Routing Point nr 230.

3. Provide message waiting

   1303 > 2xx > 0; Provide message waiting to all terminals.

4.2.7.2. Message Waiting Indication and IP DECT

To enable MWI indication on the system:

1. Program IP DECT the following way

   1303 > IP DECT number > 0
   1524/1540 > service restriction class of IP DECT number > 1

2. Disable CID CB

   15126 > service restriction of IP DECT number > 1

3. Disable message reminder

   1547/1548 > service restriction of IP DECT number > 0

4. Enable code for MWI search

   200 > A0 (= *0) >A146
   5115 > tenant number in which DECT's are > VM group number

Note that message indication on IP DECT only works when the user receives a message in the voicemail box (of the BCT client). Via BCT the user can see/play/delete voicemail messages. BCT updates the MWI lamp on the DECT set.

4.2.8. PBX configuration for the Contact Center

As stated before, the Contact Center supports both IVR less configurations (see Figure 4-3 IVR-less Contact Center example) and IVR configurations (see Figure 4-4 Contact Center with IVR/VMP lines example). The configuration for IVR less configuration is similar to the operator configuration. The IVR configuration uses the voicemail configuration. In addition, you can program login/logout facilities for agents and prompt recording.

Note: *For Contact Center only systems, there should be at least 1 Routing Point configured in Supervisor Dashboard, for parking a call during transferring the call to an agent.*

4.2.8.1. Program Contact Center with IVR less

Figure 4-3 IVR-less Contact Center example shows three Routing Points for the IVR less configuration: Service, Sales and Support. By using different Routing Points the contact center can distinguish between incoming calls for Service, Sales or Support and the agent can answer the phone appropriately.

Execute the following procedure to configure Routing Points in the PBX.

1. Program virtual numbers:

   11 > 0514 > 250; Create 'Service' access
   11 > 0515 > 251; Create 'Sales' access
   11 > 0516 > 252; Create 'Support' access

2. Define the virtual numbers as OAI monitored numbers:

   171 > 250 > 3;
   171 > 251 > 3;
   171 > 252 > 3;

3. Put all virtual numbers in their own group :

   172 > 250 > 11; group 11 for Service
   172 > 251 > 12; group 12 for Sales
   172 > 252 > 13; group 13 for Support

4. Set the OAI monitored numbers to busy out:

   E50 > 250 > 0;
   E50 > 251 > 0;
   E50 > 252 > 0;

In case the BCT server fails or the connection to the PBX is lost a Fallback configuration should be programmed. During Fallback calls to the Routing Points for Service, Sales and support are automatically rerouted to the extensions of the agents (or to subline keys on telephone sets of agents) who are then able to answer the calls.

Execute the following procedure to configure Fallback in the PBX.

1. Put the extension of the agents who provide the service in the same group as the Routing Point:

   172 > 210 > 11; agent extension 210 for Service
   172 > 211 > 11; agent extension 211 for Service
   172 > 212 > 12; agent extension 212 for Sales
   172 > 213 > 12; agent extension 213 for Sales
   172 > 214 > 13; agent extension 214 for Suppport
   172 > 215 > 13; agent extension 215 for Suppport

2. Call direction during fall back:

   170 > 250 > 210; Call direction for Service
   170 > 210 > 211;
   170 > 211 > 250;
   170 > 251 > 212; Call direction for Sales
   170 > 212 > 213;
   170 > 213 > 251;
   170 > 252 > 214; Call direction for Support
   170 > 214 > 215;
   170 > 215 > 252;

4.2.8.2. Program Contact Center with IVR

Figure 4-4 Contact Center with IVR/VMP lines example shows three access numbers for the IVR contact center; Service, Sales and Support. Calls to the access numbers are forwarded to a UCD group that contains the VMP lines. This BCT server answers the VMP lines and route the calls to agents. The VMP lines are IP DECT extensions that are subscripted by the VMP software.

Execute the following procedure to configure the IVR contact center in the PBX.

1. The UCD group with VMP lines is already configured for the voicemail configuration see: 4.2.7.1 Program VMP Lines.

2. The contact center access numbers are virtual numbers that need to be programmed with "call forwarding all calls" to the pilot number of the UCD group with VMP lines. In our example this is the pilot number 230 of the UCD group. The following example defines the access numbers from Figure 4-4 Contact Center with IVR/VMP lines example:

   Define Contact Center access numbers:

   11 > 508 > 240; Create 'Service' access.
   11 > 509 > 241; Create 'Sales' access.
   11 > 510 > 242; Create 'Support' access.

3. Set the Call Forwarding all calls from the access numbers to the UCD pilot:

   E600 > 240 > 230; CF all calls to UCD hunting group nr 230.
   E600 > 241 > 230; CF all calls to UCD hunting group nr 230.
   E600 > 242 > 230; CF all calls to UCD hunting group nr 230.

4. For the Fallback scenario, the agent extensions should be put in a separate agent group. The agent extensions are members of this agent group. When a Fallback scenario occurs, a MANUAL forwarding from the Access numbers to the Fallback group should be set with command:

   E600 > 240 > pilot of agent group for Service;
   E600 > 241 > pilot of agent group for Sales;
   E600 > 242 > pilot of agent group for Support;

   This command can be executed with a MOC terminal or on a DT-serie terminal (CAT mode).

4.2.9. Status switching of phone based agents

Agents can change their status (Logon, Logoff, Ready, Not ready and Work ready) by using one of the following methods:

1. Call a Logon Starter Line (can only be used with IVR configuration)

2. Press an agent status switch Key on the agent's phone (can only be used with DT-serie terminals)

3. Dial an agent status switch access prefix

Each method requires its own programming in the PBX.

4.2.9.1. Agent status switching using Starter Line

For Logon via a Starter Line use the following procedure to configure the PBX:

1. The UCD group with VMP lines is already configured for the voicemail configuration see: 4.2.7.1 Program VMP Lines

2. Create a virtual number for the Agent Logon starter line.

   11 > 511 > 243;

3. Set the Call Forwarding all calls from the Agent logon starter line to the UCD pilot:

   E600 > 243 > 230; CF all calls from 243 to 230

For creating the Agent Logon starter line see 8.2.5 Phone-based agents

4.2.9.2. Agent status switching using function key(s) on agents phone

For Single key agent status switching, use the following procedure to configure the PBX:

1. Program an OAI function key under a programmable key of the agent's DT-serie terminal.

   The OAI function key's start with OAI function key F1033 for programmable key1 on the DT-serie terminal until OAI function key F1047 for programmable key15. For instance, when using programmable key6 for Agent Login key then program OAI function key F1038 under programmable key6.

   9000 > extension,06 > F1038;

2. Assign an MSF operation code to the OAI function key.

   D70 > F1038 > 128;

For Multiple key agent status switching use the following procedure to configure the PBX:

1. Program an OAI function key under a programmable key of the agent's DT-serie terminal for each desired agent status. The OAI function key's start with OAI function key F1033 for programmable key1 on the DT-serie terminal until OAI function key F1047 for programmable key15. For instance, when using programmable keys 4 up to and including 8 for agent status keys then respectively program OAI function keys F1036 up to and including F1040 under programmable keys 4 up to and including 8.

   9000 > extension,04 > F1036;
   9000 > extension,05 > F1037;
   9000 > extension,06 > F1038;
   9000 > extension,07 > F1039;
   9000 > extension,08 > F1040;

2. Assign an MSF operation code to each OAI function key.

   D70 > F1036 > 128;
   D70 > F1037 > 129;
   D70 > F1038 > 130;
   D70 > F1039 > 131;
   D70 > F1040 > 132;

Note: *To avoid confusion with Operation Codes as mentioned in the PBX Command Manual: please make sure you use the codes mentioned above (128-132)*

4.2.9.3. Agent status switching using one or more access prefix(es)

For Single agent status switching access prefix use, the following procedure to configure the PBX:

1. Assign an access prefix for OAI in the number plan.

   200 > access prefix > A084;

2. Assign a MSF operation code to this access prefix.

   D71 > access code > 128;

3. To allow MSF operation on the station:

   1202 > station > ClassA-ClassB Assign the station to a certain Service restriction class B
   15059> Class B > 0 allow the station in Class B to use OAI-MSF by using access prefix

For multiple agent status switching access prefixes use the following procedure to configure the PBX:

1. Assign an access prefix for OAI for each agent status prefix in the number plan.

   200 > access prefix > A084;
   200 > access prefix > A084;
   200 > access prefix > A084;
   200 > access prefix > A084;
   200 > access prefix > A084;

2. Assign a MSF operation code to each access prefix.

   D71 > access code > 128;
   D71 > access code > 129;
   D71 > access code > 130;
   D71 > access code > 131;
   D71 > access code > 132;

3. To allow MSF operation on the station:

   1202 > station > ClassA-ClassB Assign the station to a certain Service restriction class B
   15059 > Class B > 0 allow the station in Class B to use OAI-MSF by using access prefix

Note: *To avoid confusion with Operation Codes as mentioned in the PBX Command Manual: please make sure you use the codes mentioned above (128-132)*

4.2.10. Codes for phone based agents

Phone based agents use codes to identify the desired status when a single function key or access prefix is defined. Entering status information is only applicable for Phone Based Agents. When the steps in 4.2.9 Status switching of phone based agents have been entered it is possible to use this feature.

The following codes are defined:

- 0# to logon
- 1# to logoff
- 2# to switch Not Ready
- 3# to switch Ready
- 5# to switch Work ready, leaving the after call work

In case the required agent status is logged-on, a PIN is requested to identify the agent. For information on how to configure a phone based agent with PIN in BCT see 8.5.10 Manually create a BCT user – the Agent by Phone parts.

In case the required agent status is not ready, a Not Ready Reason (NRR) is requested to identify why the agent is switched not ready. Not Ready Reasons (NRR) are entered in tables in the Business ConneCT Database via BCT Supervisor Dashboard. The information in the **Dial Code** column references the chosen Additional Info digits. After installation, a number of default NRRs are available in the chosen system language. In this example the English NRRs are given with their default dial codes:

Not Ready Reason	Dial Code
Coffee break	1
Lunch	2
Other work	3
Personal affairs	4

For more information on how to configure Not Ready Reasons in BCT, see chapter “Not Ready Reasons” in BCT Administrator Guide.

In case the required agent status is ready, a Call Type (CT) is requested to identify the type or outcome of the handled call. Call Types (CT) are entered in the Business ConneCT database via BCT Supervisor Dashboard. The information in the Dial Code column references the chosen Additional Info digits. After installation, a number of default CTs are available in the chosen system language. In this example the English CTs are given with their default dial codes:

Call Type	Dial Code
Successful	1
Unsuccessful	2

For more information on how to configure Call Types in BCT, see chapter “Call Types” in BCT Administrator Guide.

***Note:** A code is always terminated with a # !*

4.2.11. Prompt Recording

In the callflow for the Contact Centre prompts can be played to welcome the customer, to present an office message for the Clock module, to select options from Attendant menus etc. To record these prompts a Starter Line has to be defined. This Starter Line is a virtual number that is programmed with "call forwarding all calls" to the pilot number of the UCD group with VMP lines.

To program this Starter Line use the following procedure to configure the PBX:

1. The UCD group with VMP lines is already configured for the voicemail configuration see: 4.2.7.1 Program VMP Lines

2. Create a virtual number for the Prompt Recorder Starter Line.

   11 > 512 > 244;

3. Set the Call Forwarding all calls from the Prompt Recorder Starter Line to the UCD pilot:

   E600 > 244 > 230; CF all calls from 244 to 230

4.2.12. PBX configuration for the special monitored number

To ensure that call handling and call transfer works in all cases, you must configure a special Monitored number. This number is needed for various situations, such as enabling Contact Center agents to transfer calls to other agents, and ending unanswered ISDN calls (by providing a place to park the calls first).

Configure the special Monitored number as follows:

11 > 513 > 296;	Create virtual Queue
E50 > 296 > 0;	Make number busy
171 > 296 > 3;	Define virtual number as OAI Monitored number for BCT
172 > 296 > 15;	Put in group

4.2.13. Open number scheme

Supported for SV8300 networks and SV9300 networks
Not supported for any other mixed networks e.g. SV8300/SV9300 networks.

4.2.14. Multi-line

SV8300/SV9300

Define Virtual extensions, to be used as Sub Lines, in the PBX with command 11.

Define the Sub Lines as keys on the DT-serie terminals with command 9000.

BCT System Settings

Check Enable Multi Line in Connection Tab for the PBX (edit PBX page).

Check Enable Multi Line when editing Advanced User Settings in Company Directory for the users using Multi Line.

Synchronize BCT.

BCT Client

When now a BCT-client is started, the line-view can be selected and the list of lines is displayed in the same order as the buttons are used on the terminal.

For User settings for Lines, enter the configuration page and select the Lines tab.

4.2.15. Mobility Access

Implement Trunkbased Mobility Access according to the programming manual of the SV8300/SV9300.

To make call forward setting overrule the MA forwarding, the following need to be programmed:

15484>RestrictionClass C > 0; Priority for Call Forwarding-All Calls of Mobility Access call

The Restriction Class C should be the Class C that the MA extensions are assigned to (with command 1207). BCT synchronization should be executed after programming the MA extension.

Check via System Settings / Company Directory / Extension info that the Detected Terminal Type is Mobile/SMA extension. If not, use "Manual Terminal Type" to override.

The BCT Desktop Client can be used for presence profile configuration.
The BCT Mobility Client should be used for call handling.

4.2.16. Suite Room

When Suite Room is configured, when the room (Master phone) is called all phones will ring.

To configure Suite Room:
Suppose that room number 000 has phone 100, 101 and 102. 100 is the master phone, 101 and 102 are slave phones.

1. Set correct OAI mode:

   ```
   08 > 1602 > 0;
   ```

2. Set Master and Slave

   ```
   1278 > 100 > 0; // Master
   1278 > 101 > 1; // Slave
   1278 > 102 > 1; // Slave
   ```

3. Define room

   ```
   1279 > 100 > 000; // Room
   1279 > 101 > 000; // Room
   1279 > 102 > 000; // Room
   ```

4. Define room position

   ```
   5734 > 00000 > 100;
   5734 > 00001 > 101;
   5734 > 00002 > 102;
   ```

5. Send Busy Tone when either station is busy.

   ```
   1202 > 100 > 1415;          // Service Restriction Class of Master Station = 14
   15227 > 14 > 1;             // Send Busy Tone when either station is busy
   ```

Notes: *- A Suite Room phone should not be combined with a BCT client. Extension status information will not be shown. In a hotel environment usually the operator is using a BCT client and the operator should not be based on a Suite Room extension.*
- BCT Operator will see extension status of the master extension in a Suite Room configuration
- SV8300/SV9300 minimal R8.2 is required for Suite Room Support in BCT

4.3. UNIVERGE SV8500/SV9500 configuration

This chapter explains how to set up the PBX types SV8500/SV9500 for BCT for a single node configuration, a FCCS network or a SV9500 Geographic redundant network. When BCT is running and you make changes in the PBX configuration that have impact on BCT, you may have to restart UCS Runtime (see 4.1.6 Restart of UCS Runtime).

You program the PBX with the MA4000 and/or MAT/PCPro application.

Please refer to the Field Change Order to check the PBX compatibility.

4.3.1. SV8500/SV9500 Preconditions and differences

Programming all systems is the same. Only the correct PBX should be selected when BCT makes a connection.

SV8500/SV9500

For SV8500/SV9500, Location Diversity is supported. See 4.3.1 SV8500/SV9500 configuration for location diversity

WARNING: *In case of an SV8500/SV9500 you need to check SVI 1371. When BCT is used on SV8500/SV9500, SVI 1371 needs to be set to 1 (otherwise, synchronization will fail on stand-alone SV8500/SV9500 systems).*

Note: *When SVI 1371 is 0, please contact your (local) supplier. There is a license mismatch in SV8500/SV9500.*

Note that the SV8500/SV9500 has two LAN interfaces: LAN1 and LAN2. When configuring BCT for an SV8500/SV9500 PBX, the **LAN2 (ACT) IP address** must be assigned.

BCT uses MAT commands to connect to the SV9500 and retrieve the PBX configuration. From SV9500 version 8.0 and onwards it is mandatory to connect to the SV9500 by using a User account. This User account needs sufficient privileges to execute MAT commands. The MAT commands are grouped in related commands and these groups can be enabled (allowed) to Login Grades. The Login Grade can then be assigned to a User account to connect to the PBX.

The groups of MAT commands that BCT uses to connect to the SV9500 and retrieve the PBX configuration are:

- System Control
- Service Feature Data
- List Up Commands(1) - > List Up Station data
- List Up Commands(2) - > List Up Local Data Memory
- List Up Commands(2) - > List Up Network Data Memory
- List Up Commands(2) - > List Up Hotel/Motel (not for Busienss mode)
- List Up Commands(2) - > List Up OAI
- List Up Commands(2) - > List Up SIP Service

- Installation
- Local Data Memory
- Network Data Memory

So a Login grade needs to be defined with the above mentioned groups of MAT commands and this Login grade must be assigned to a dedicated User account used by BCT to connect to the PBX.

To create a User account for BCT user the PCpro application:

- Connect to the SV9500 with a System Manager account.
- Go to menu User and select Login Grade Settings.
- In Login Grades Settings (left pane) select a Login Grade from the Login Grade List.
- In Executable Commands (right pane) enable the above groups of MAT commands.
- Press Setup to create the Login Grade and press OK to confirm.
- Back in PCpro go to menu User and select User Account Setting.
- In User Account Settings press Add.
- Enter a User ID, leave Data Memory to option LDM, enter and confirm a Password and select the above created Login grade from the drop down list.
- Press Setup to create the User account and press OK to confirm
- Press Close in User Account Setting.

The created User account (User ID and password) can then be used in the BCT to configure the PBX of type SV9500, see 8.1.1 Using the Configuration Wizard or 8.1.5 Connection to PBX.

In case of SV8500/SV9500 in a FCCS network, the nodes must be assigned manually to a configuration file:

- Open the configuration file "PBXConfigurationService.WinService.exe.config" in "C:\Program Files (x86)\Common Files\NEC\Services" with notepad. Look for the section "fusionSettings".
- A part of the configuration file looks like:

```
</configuration>
  ...
  <fusionSettings>
    <!-- For each node in the fusion network add a new key value entry -->
    <!--  key   = FPC (Fusion Point Code)         -->
    <!--  value = MAT IP address                  -->
    <!-- Example:                                 -->
    <!-- <add key ="2" value="192.168.111.52"/>   -->
    <!-- <add key ="3" value="192.168.111.123"/>  -->
  </fusionSettings>
</configuration>
```

- You only have to configure the nodes. The NCN (Network Control Node) with FPC = 1 can be left out. The FPCs must be unique, but that is always the case in an FCCS network.

- The tags "<!--" en "-->" define the line to be comment, so this has to be removed.

- Example of a configured network:

```
<fusionSettings>
   <add key ="2" value="192.168.111.52"/>
   <add key ="3" value="192.168.111.123"/>
</fusionSettings>
```

4.3.2. PBX boundaries, options and licenses single node and FCCS

Make sure the following ASYD/ASYDL settings are present. To read and change settings, use the PCPro commands ASYD/ASYDL.

ASYD	SYS 1 INDEX 27	bit 6	must be ‘0’	OAI Message Type
ASYD	SYS 1 INDEX 31	byte=	0x06	CM Mounting capacity
ASYD	SYS 1 INDEX 32	bit 1	must be ‘1’	Record Tenant Data for SMDR/CS Report
ASYD	SYS 1 INDEX 32	bit 2	must be ‘1’	Record Selected Trunk type for SMDR/CS Report
ASYD	SYS 1 INDEX 32	bit 7	must be ‘1’	SMDR/CS Report in service
ASYD	SYS 1 INDEX 47	bit 4	must be '1'	Tone control via SFC (FN=127)
ASYD	SYS 1 INDEX 63	bit 6	must be '1'	Enable ‘Original called number in OAI event in case of DDI fail routed call via CCIS’
ASYD	SYS 1 INDEX 63	bit 7	must be '0'	SPACD out of Service
ASYD	SYS 1 INDEX 69	bit 0	must be '0'	Return transferred call to transferring party after Recall Timer expires
ASYD	SYS 1 INDEX 78	bit 0	must be '1'	Intermediate Station Number Display
ASYD	SYS 1 INDEX 78	bit 3	must be '1'	Dial Number Display
ASYD	SYS 1 INDEX 78	bit 5	must be '1'	Name Display Service
ASYD	SYS 1 INDEX 79	bit 2	must be '0'	Split Call Forwarding Services **Note:** when changing this setting please verify the Call Forwarding relations again!
ASYD	SYS 1 INDEX 79	bit 5	must be '1'	Expanded Name Display (16-digit)
ASYD	SYS 1 INDEX 79	bit 6	must be '0'	OAI in Service
ASYD	SYS 1 INDEX 92	byte=	0x3F	Common tenant data table
ASYD	SYS 1 INDEX 93	byte=	0xBF	Common tenant data table
ASYD	SYS 1 INDEX 94	Byte=	0x08	Common tenant data table
ASYD	SYS 1 INDEX 207	bit 0	must be '1'	IP0 is used
ASYD	SYS 1 INDEX 241	bit 1	must be '1'	Name Display (16-digit)
ASYD	SYS 1 INDEX 241	bit 2	must be '1'	Call Processing Event Notification
ASYD	SYS 1 INDEX 241	bit 3	must be '1'	Detail Info on SCF Error
ASYD	SYS 1 INDEX 241	bit 7	must be '1'	OAI/SSFN

ASYD	SYS 1 INDEX 370	bit 0	must be '1'	Expanded SMFN Service
ASYD	SYS 1 INDEX 370	bit 4	must be '0'	Release Guard Timer for Single Line
ASYD	SYS 1 INDEX 370	bit 5	must be '0'	MTC=0x15 ms
ASYD	SYS 1 INDEX 370	bit 6	must be '0'	MTCx64 ms
ASYD	SYS 1 INDEX 370	bit 7	must be '0'	Default 384 ms
ASYD	SYS 1 INDEX 449	bit 0	must be '1'	Send OFF_HOOK when executing OAI MakeCall
ASYD	SYS 1 INDEX 512	byte=	0x01	OAI on NCN
ASYDL	SYS 1 INDEX 514	byte=	Not equal to 0x00	Amount of NDM memory, for instance 0x01 (2MB), 0x03 (4Mb)
ASYDL	SYS 1 INDEX 533	byte=	0x01	FPC of VNDM (VNDM is holding the OAI link to the BCT server)
ASYDL	SYS 1 INDEX 810	bit 0	must be '1'	PHC Music-on-Hold source is self office
ASYDL	SYS 1 INDEX 864	bit 0	must be '1'	Build in IP is provided
ASYDL	SYS 1 INDEX 864	bit 2	must be ‘0’	Agent Anywhere/OAI Terminal Anywhere (SVI 1761)
ASYDL	SYS 1 INDEX 864	bit 3	must be ‘0’	Multiple OAI/ACD In-Service (SVI 1265)
ASYDL	SYS 1 INDEX 864	bit 4	must be '1'	8-port monitoring
ASYDL	SYS 1 INDEX 864	bit 5	must be '0'	Clear Status Monitor Facility Notification (SMFN) when the FCCS link is down
ASYDL	SYS 1 INDEX 865	byte=	0x01	FPC of node providing IP
ASYDL	SYS 1 INDEX 867	bit 0	must be '1'	Expanded SMFN
ASYDL	SYS 1 INDEX 867	bit 1	must be '0'	IP1 is not used
ASYDL	SYS 1 INDEX 867	bit 3	must be '1'	Improvement of SCF6 Request for Monitor Connection
ASYDL	SYS 1 INDEX 867	bit 4	must be '1'	FLF Facility number length and logical number length (Must be set the same in all nodes)
ASYDL	SYS 1 INDEX 867	bit 7	must be '1'	16-digit Station Number
ASYDL	SYS 1 INDEX 869	bit 4	must be '1'	Activate OAI events in case of recalling failed transferred call
ASYDL	SYS 1 INDEX 874	bit 2	must be '1'	SMFN 12 (SMFR 139)
ASYDL	SYS 1 INDEX 874	bit 4	must be '1'	Camp On Transfer CCIS (OAI)
ASYDL	SYS 1 INDEX 874	bit 7	must be '1'	Break-in CCIS (OAI)
ASYDL	SYS 1 INDEX 875	bit 0	must be '0'	OAI SMFN FN9 STS=01 notification
ASYDL	SYS 1 INDEX 875	bit 1	must be '1'	OAI SMFN FN9 STS=02, 03 notification
ASYDL	SYS 1 INDEX 875	bit 2	must be '1'	Callback, Outgoing Trunk Queuing, Callback-CCIS
ASYDL	SYS 1 INDEX 875	bit 3	must be '1'	Break-in – local DND override

ASYDL	SYS 1 INDEX 876	byte=	0x02	Adjust wait time for guarding case of busy of SCF7(transfer facility)
ASYDL	SYS 1 INDEX 878	bit 1	must be '1'	Timer SCF7 (Transfer) on 180 Ringing for PHS/WLAN/St.SIP destination.
ASYDL	SYS 1 INDEX 895	bit 5	must be '1'	Call back destination starts ringing after initiator answers call back
ASYDL	SYS 1 INDEX 1187	bit 6	must be '1'	OAI support ETSI Addressing
ASYDL	SYS 1 INDEX 1188	Bit 0	must be '1'	Calling party number selection function with SCF
ASYDL	SYS 1 INDEX 1188	Bit 1	must be '1'	Extended function of SCF (FN=128)
ASYDL	SYS 1 INDEX 1188	Bit 5	must be '1'	Number of Concurrent Connections for Predictive Dialing
ASYDL	SYS 1 INDEX 1188	Bit 6	must be '1'	OAI call kind
ASYDL	SYS 1 INDEX 1200	Bit 6	must be '0'	Registered terminal info

If settings are incorrect, start monitor on OAI will produce error 0x01020002 "function not supported" in Diag@Net.

These settings are necessary to send the correct events over the OAI link to BCT.

WARNING: *The BCT server uses an OAI connection to communicate with a PBX. A SV8500/SV9500 can handle A MAXIMUM OF 8 (DEFAULT) OAI connections.*

WARNING: *For queue mapping, monitored numbers are assigned in a PBX. In the PBX one monitored number can be used by max. 8 applications. ADVICE: Do not use the same monitored number for different applications.*

Licenses

Make sure you have the following:

- ‘Option OAI’ license;
- Sufficient IP capacity licenses;
- Sufficient IP terminal port licenses (if using VMP IVR);

4.3.3. PBX boundaries, options and licenses dedicated for FCCS

The following system options are dedicated for FCCS networks. These settings go ‘on top’ of the settings mentioned in the previous section. In case certain options mentioned in the next table overlap with the previous table, be sure to stick to the settings described below.

Consider the following FCCS network:

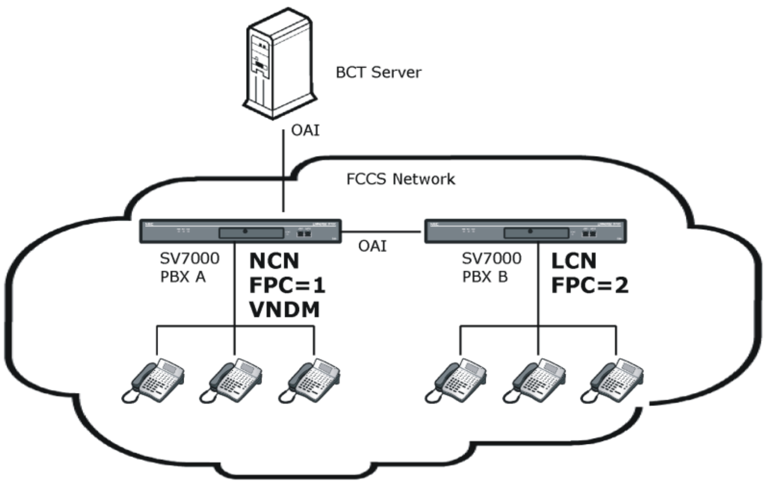


Figure 4-7 FCCS network

For PBX-A (NCN):

ASYDL	SYS 1 INDEX 533	byte=	0x01	FPC of VNDM (VNDM is holding the OAI link to BCT server)
				Set the MDATA parameter to 0xFF to program the ASYDN value as well.
ASYDL	SYS 1 INDEX 864	bit 0	must be '1'	Build in IP is used
ASYDL	SYS 1 INDEX 864	bit 2	must be '1'	Agent Anywhere/OAI terminal anywhere
ASYDL	SYS 1 INDEX 865	byte=	0x01	FPC of node providing IP

For PBX-B (LCN):

ASYD	SYS 1 INDEX 207	bit 0	must be ‘0’	IP0 is not used
ASYD	SYS 1 INDEX 207	bit 1	must be ‘0’	IP1 is not used
ASYDL	SYS 1 INDEX 533	byte=	0x01	FPC of VNDM (VNDM is holding the OAI link to BCT server)
				Set the MDATA parameter to 0xFF to program the ASYDN value as well.
ASYDL	SYS 1 INDEX 864	bit 0	must be '0'	Build in IP is not used
ASYDL	SYS 1 INDEX 864	bit 2	must be '1'	OAI terminal anywhere
ASYDL	SYS 1 INDEX 865	byte=	0x01	FPC of node providing IP

Note that this is an example with two FCCS nodes. In case there are more nodes in the networks, the settings for LCN have to be programmed in every LCN. Please also take notice of the PBX system documentation: DPG(win) OAI, section OAI FCCS single IP configuration and OAI FCCS data programming (table 5-1).

Licenses

Make sure you have the following OAI licenses

- 'Option OAI' license;
  Note: for SV9500 it is for free and will be automatically generated.
- 'Option NET OAI ACD' license.

4.3.4. Extended ISDN addressing (Rel. S05 or higher)

When using extended addressing (ASYDL/N, system 1, index 1088, bits 5 and 6 set to 1 [x60]) it is not only necessary to put ISDN trunkroutes and stations in local domains using ADLDL/N, but also monitored numbers (including special monitored number), other starterline numbers (IVR based starters), the ACFON destination number and all VMP lines need to be assigned to a defined local domain. If this is not the case, BCT will be confronted with OAI messages that do not comply with the extended addressing format (e.g. TAC's may be missing and such).

When old style ISDN addressing is used (ASYDL/N, system 1, index 1088, bits 5 and 6 set to 0 [x00]), the above does not apply.

For details about programming (special) monitored numbers, VMP lines, starter lines and ACFON destination number please read the sections below.

4.3.5. PBX configuration for the operator

The following picture shows Operator Routing Points.

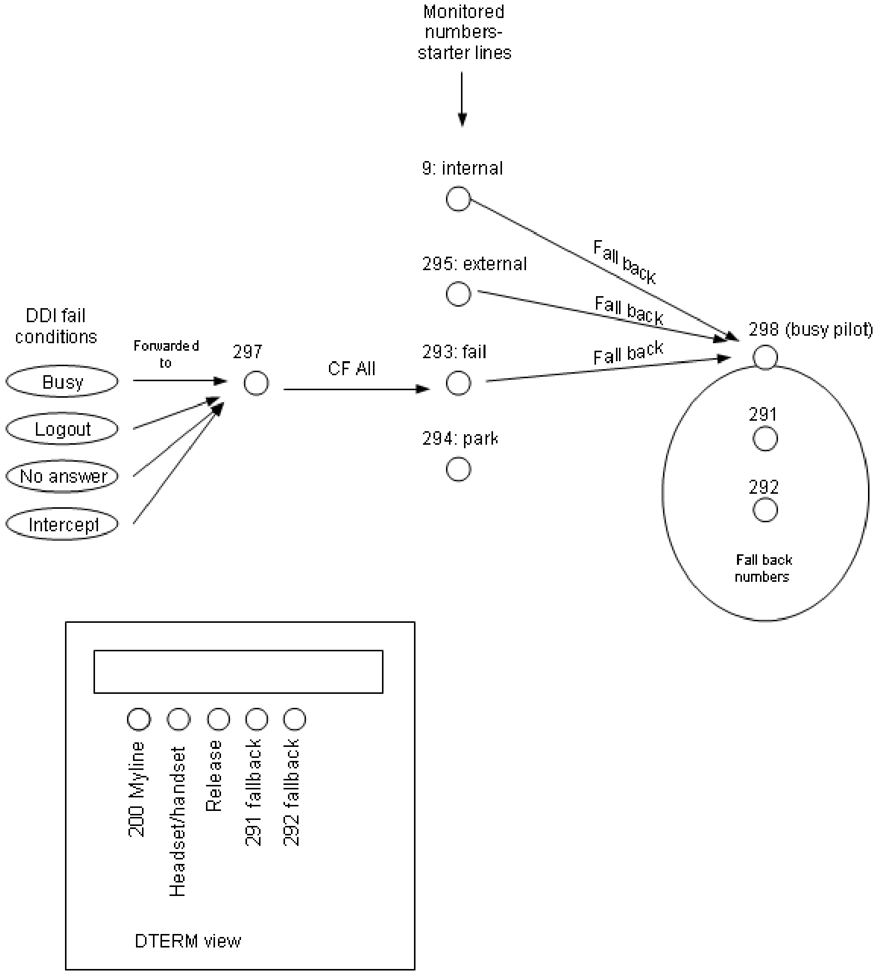


Figure 4-8 Operator routing points

Choice of numbers:

- Starter Lines:
  9: internal
  295: external (general DID number)
  293: failed
  294: park
- 200: Myline of the Operator Dterm
- 291: Subline number for Fallback when server is down
- 292: Subline number for Fallback when server is down
- 260 to 262: System Call Park (also called Pickup Park)

Actions:

1. Define your numbering plan with the ANPDN and ASPAN commands. Make sure that all used numbers are in the number plan.

   ```
   ANPDN TN=1, 1stDC=2, CI=N/B/H, NND=3, BLF=0
   ANPDN TN=1, 1stDC=9, CI=N/B/H, NND=1, BLF=0
   ASPA TN=1, ACC=2, CI=N/B/H, SRV=STN
   ASPAN TN=1, ACC=2, CI=N/B/H, SRV=TELN, NND=3
   ASPAN TN=1, ACC=9, CI=N/B/H, SRV=TELN, NND=1
   ```

Note: *Each of the above commands needs to be assigned two times: once for CI (Connection Status Index) and once for CI Hooking.*

2. Create a Fallback group. Failed calls are routed to the operator via OAI Monitored numbers.

   ```
   ASDT TN=1, STN=291, LEN=073240, TEC=18, RSC=1, SFC=1
   ASDT TN=1, STN=292, LEN=073241, TEC=18, RSC=1, SFC=1
   ASDT TN=1, STN=298, LEN=073242, TEC=18, RSC=1, SFC=1
   ALGSN TYPE=2, UGN=1, TELN=291, FPC=1, TN=1, STN=291
   ALGSN TYPE=2, UGN=1, TELN=292, FPC=1, TN=1, STN=292
   ALGSN TYPE=2, UGN=1, TELN=298, FPC=1, TN=1, STN=298
   ASHUN UGN=1, TELN=298, EDIT TELN: 291+292 (press sort all and set)
   ```

   Add queuing to this group (in this example, 10 callers can be queued):

   ```
   AUCDN UGN=1, TELN=298, QTHACT=1, QTH=10, CWT=10, MCI=0
   ```

   Make the pilot number of the group busy:

   ```
   MBST TN=1, STN=298, MB=1
   ```

3. Define OAI Monitored numbers.

   First create TELN numbers:

   ```
   ALGNN, UGN=1, TELN=9
   ALGNN, UGN=1, TELN=295
   ALGNN, UGN=1, TELN=293
   ALGNN, UGN=1, TELN=294
   ```

   Create Monitored numbers:

   ```
   AMNON A/G=Administrative station, UGN=1, N_MNO=9,     N_NMI=1, MFC=0, check mark
   "Follow the UCD when monitor status is not requested from AP”, TELN= 298
   AMNON A/G=Administrative station, UGN=1, N_MNO=295, N_NMI=2, MFC=0, check mark
   “Follow the UCD when monitor status is not requested from AP:, TELN= 298
   AMNON A/G=Administrative station, UGN=1, N_MNO=293, N_NMI=3, MFC=0, check mark
   “Follow the UCD when monitor status is not requested from AP”, TELN= 298
   AMNON A/G=Administrative station, UGN=1, N_MNO=294, N_NMI=4, MFC=0, no check mark
   “Follow the UCD when monitor status is not requested from AP”
   ```

4. Define the operator Dterms prime and subline:

   AISTL TN=1, IP STN=200, KIND=DTERM IP, TEC=12, RSC=1, SFC=1, LEN=073000
   AKYD TN=1, STN=200, PRI=2, PL TN=1, PL STN=200, S=1, MWD=0, LN PRE=1, SPK=1, ANS=2, ORG=0, TP=0
   ALGSN TYPE=2, UGN=1, TELN=200, FPC=1, TN=1, STN=200

   In the table that appears:
   KYN= 1, KYI=2, KD=0, TN=1, STN=200, RG=7 Myline Operator
   KYN= 2, KYI=1, FKY=56, Headset (LED on) / handset key (LED off)
   KYN= 5, KYI=1, FKY=59, Release key (this setting might be skipped)
   KYN= 6, KYI=2, KD=0, TN=1, STN=291, RG=7 Assigns fallback station 291 as subline to operator DTERM
   KYN= 7, KYI=2, KD=0, TN=1, STN=292, RG=7 Assigns fallback station 292 as subline to operator DTERM

5. Define DDI fail actions:

   Program the number to which failed calls should be routed first
   ASDT TN=1, STN=297, LENS=073243, TEC=18, RSC=1, SFC=1
   ALGSN TYPE=2, UGN=1, TELN=297, FPC=1, TN=1, STN=297
   Set CF No Answer for 297 to the Monitored number 293
   ACFS_T TN=1, TELN=297, press Get, select radio buttonTYPE = ‘Call Forwarding’ and SRV = ‘Don't Answer'.

   Program the fail actions to be forwarded to 297:
   ACFON TN=1, CF Busy Line, CFI=TELN, UGN=1, TELN=297
   ACFON TN=1, CF Don’t Answer, CFI=TELN, UGN=1, TELN=297
   ACFON TN=1, CF Intercept, CFI=TELN, UGN=1, TELN=297
   ACFON TN=1, CF Logout, CFI=TELN, UGN=1, TELN=297
   ACFON TN=1, CF Incomplete Number, CFI=TELN, UGN=1, TELN=297
   ACFON TN=1, CF Not Reach, CFI=TELN, UGN=1, TELN=297 (note: since SV8500/SV9500 S5)

   In case ACFON Intercept (Number Unobtainable) is required, keep in mind that the incoming Route for which the DDI fail actions are applicable, ARTD(N) CDN 43 (BT) gives following behavior:
   CDN 43 = 0, ACFON Intercept will be followed to route an incoming call with incorrect (NU) called party number
   CDN 43 = 1, Call is released with ISDN cause "Unallocated Number

6. Shorten the CFNA timers for 297 to improve rerouting time to operator for external calls to busy extensions:

   ADAI_T MODE select radio button MODE=TELN, enter UGN=1 TELN=297, then press Get, then enter for CDN value 7 (139TC) the value of 1. All other CDNs must be left at value 0. Press Set.

7. To use the System Call Park functionality for operators (also called Pickup Park) a separate set of OAI monitored numbers need to be programmed. For every System Call Park position OAI monitored numbers need to be created.

First create TELN numbers:

```
ALGNN, UGN=1, TELN=260
ALGNN, UGN=1, TELN=261
ALGNN, UGN=1, TELN=262
```

Create Monitored numbers:

```
AMNON A/G=Administrative station, UGN=1, N_MNO=260, N_NMI=2, MFC=0
AMNON A/G=Administrative station, UGN=1, N_MNO=261, N_NMI=2, MFC=0
AMNON A/G=Administrative station, UGN=1, N_MNO=262, N_NMI=2, MFC=0
```

The numbers 260, 261 and 262 will now be seen as routing points by BCT and can be used for System Call Park. For BCT configuration for System Call Park see 8.3.10 Create System Call Park configuration.

4.3.6. PBX configuration for a Contact Center

Note: *For Contact Center only systems, there should be at least 1 Routing Point configured in Supervisor Dashboard, for parking a call during transferring the call to an agent.*

4.3.6.1. Program an IVR-less contact center

The following picture shows Contact Center Routing Points:

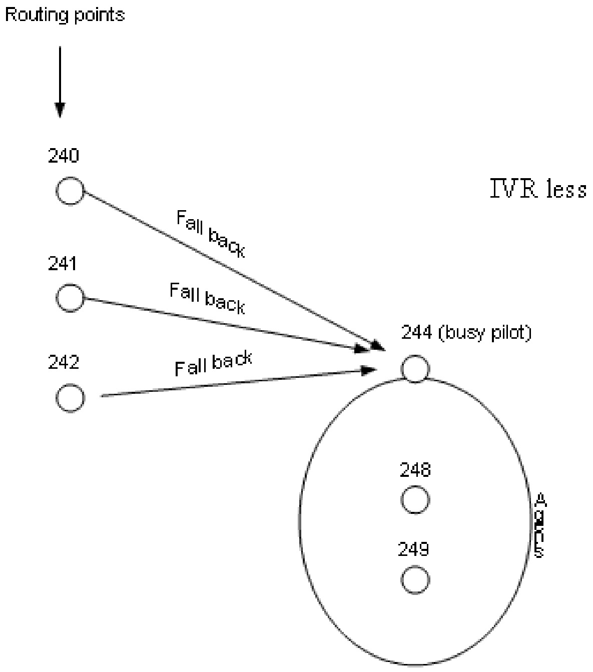


Figure 4-9 Example of IVR-less routing points

Actions:

1. Create the Fallback group for if the application fails (agents 248 and 249 are in the Fallback group):

```
ASDT TN=1, STN=244, LEN=073244, TEC=18, RSC=1, SFC=1
ALGSN TYPE=2, UGN=1, TELN=244, FPC=1, TN=1, STN=244
```

Make the pilot number of the group busy:
MBST TN=1, STN=244, MB=1

Create the group:
ASHUN UGN=1, TELN=244, EDIT TELN: 248 and 249 (press sort all and set)

Add queuing to this group:
AUCDN UGN=1, TELN=244, QTHACT=1, QTH=10, CWT=10, MCI=0

2. Create the Routing Points for the Contact Center, with Fallback option:

ALGNN, UGN=1, TELN=240
ALGNN, UGN=1, TELN=241
ALGNN, UGN=1, TELN=242

AMNON A/G=Administrative station, UGN=1, N_MNO=240, N_NMI=5, MFC=0, check mark "Follow the UCD when monitor status is not requested from AP", TELN= 244
AMNON A/G=Administrative station, UGN=1, N_MNO=241, N_NMI=6, MFC=0, check mark "Follow the UCD when monitor status is not requested from AP", TELN= 244
AMNON A/G=Administrative station, UGN=1, N_MNO=242, N_NMI=7, MFC=0, check mark "Follow the UCD when monitor status is not requested from AP", TELN= 244

Note: *If you want to use the Fallback agents, then you must program the numbers 248 and 249 as sublines on a DTERM, in the same way as done for the operator.*

4.3.6.2. Program a Contact Center with VMP IVR lines

The following picture shows Contact Center (with IVR) Routing Points:

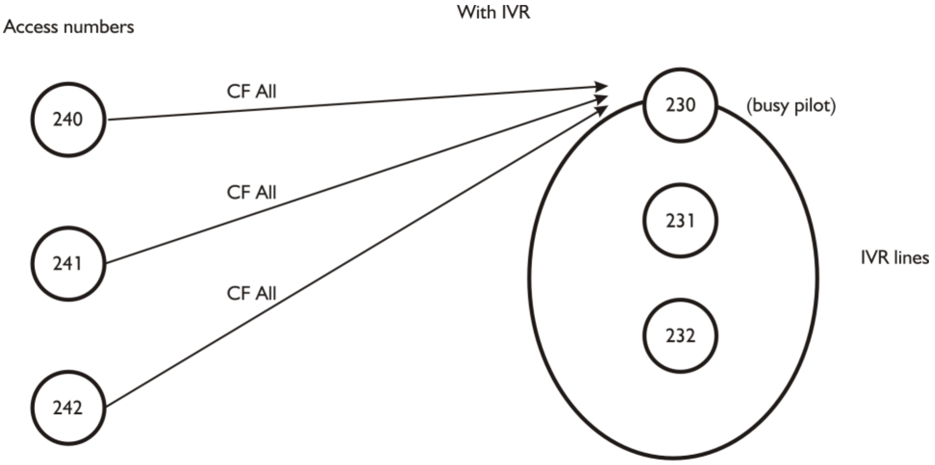


Figure 4-10 Example of routing points with VMP IVR lines

Actions:

1. Assign 2 IP DECT using command AISTL and assign TELN numbers using ALGSN:

AISTL TN=1, IP STN=231, KIND=DTERM IP, TEC=12, RSC=1, SFC=1, LEN=073001, click Set
AISTL TN=1, IP STN=232, KIND=DTERM IP, TEC=12, RSC=1, SFC=1, LEN=073002, click Set

AKYD TN=1, STN=231, PRI=0, PL TN=1, PL STN=231, S=0, MWD=0,
LN PRE=0,TP=0

In the table that appears:
KYN= 15, KYI=1, FKY=142, Logout key (in all nodes)
KYN= 16, KYI=2, KD=0, TN=1, STN=231, RG=7, Myline key (in all nodes)
AKYD TN=1, STN=232, PRI=0, PL TN=1, PL STN=232, S=0, MWD=0,
LN PRE=0,TP=0

In the table that appears:
KYN= 15, KYI=1, FKY=142, Logout key (in all nodes)
KYN= 16, KYI=2, KD=0, TN=1, STN=232, RG=7, Myline key (in all nodes)
ALGSN TYPE=2, UGN=1, TELN=231, FPC=1, TN=1, STN=231
ALGSN TYPE=2, UGN=1, TELN=232, FPC=1, TN=1, STN=232

2. Create the access numbers that are forwarded to the UCD group containing the VMP lines for playing prompts:

ASDT TN=1, STN=240, LEN=073245, TEC=18, RSC=1, SFC=1
ASDT TN=1, STN=241, LEN=073246, TEC=18, RSC=1, SFC=1
ASDT TN=1, STN=242, LEN=073247, TEC=18, RSC=1, SFC=1

ALGSN TYPE=2, UGN=1, TELN=240, FPC=1, TN=1, STN=240
ALGSN TYPE=2, UGN=1, TELN=241, FPC=1, TN=1, STN=241
ALGSN TYPE=2, UGN=1, TELN=242, FPC=1, TN=1, STN=242

ASDT TN=1, STN=230, LEN=073251, TEC=18, RSC=1, SFC=1
ALGSN TYPE=2, UGN=1, TELN=230, FPC=1, TN=1, STN=230
MBST TN=1, STN=230, MB=1
ASHUN UGN=1, TELN=230, EDIT TELN: 231+232 (press sort all and set)

ACFS_T TN=1, TELN=240, press Get, select radio buttonTYPE = ‘Call Forwarding’ and SRV = ‘All Calls’. Fill in for CFD 230 then press Set and Exit.
ACFS_T TN=1, TELN=241, press Get, select radio buttonTYPE = ‘Call Forwarding’ and SRV = ‘All Calls’. Fill in for CFD 230 then press Set and Exit.
ACFS_T TN=1, TELN=242, press Get, select radio buttonTYPE = ‘Call Forwarding’ and SRV = ‘All Calls’. Fill in for CFD 230 then press Set and Exit.

4.3.6.3. Barge-in and monitoring

In SV9500, supervisors may be allowed to silently monitor the conversation of a routed call. To get silent monitor working with all types of terminals the next setting is required:

ASYDL SYS1 Index 874 Bit 0 = 1 (Enable multi path monitor connection)
ASYDL SYS1 Index 679 Bit 1 = 1 (Multiple session for SIP Multi-Line terminal enabled)

The affected IP terminals should be re-registered afterwards.

Note that this can have legal implications, as in some countries it is not allowed to monitor silently.

4.3.7. Status switching of phone based agents

Agents can change their status (Logon, Logoff, Ready, Not ready and Work ready) by using one of the following methods:

1. Call an agent status switch Starter Line (can only be used with IVR configuration)

2. Press an agent status switch Key on the agent's phone (can only be used with (IP-)Dterm extensions)

3. Dial an agent status switch access prefix

Each method requires its own programming in the PBX.

4.3.7.1. Agent status switching using Starter Line

For agent status switching via a Starter Line use the following procedure to configure the PBX:

1. Program the access number of the Agent Logon Starter Line. See 4.3.6.2 Program a Contact Center with VMP IVR lines.

2. For creating the Agent Logon starter line within BCT, see 8.2.5 Phone-based agents

4.3.7.2. Agent status switching using function key(s) on agents phone

For Single key agent status switching use the following procedure to configure the PBX:
Program an OAI Function Key to a specific function key of the agents DTerm using command AKYD.
The OAI Function Keys range from 34 until 48 and are related to OAI Key Codes 1 until 14.
In the second step use command AOKC to map the MSF operation code to the OAI Function Key related OAI Key Code. For more information, please refer to the PBX command manual.
Below an example to assign MSF code 128 to function key 6 on extension 2000 is given:

```
AKYD, TN=1, STN=2000, PRI=0, PL TN=1, PL STN=2000, S=0, MWD=0, LN PRE=0, TP=0
KYN 6, KYI=1, FKY=34 [OAI Key Code 1 ]
AOKC, KEY-CODE=1, F-KIND=1, C-TONE=1, OP-CODE=128
```

For Multiple key agent status switching use the following procedure to configure the PBX:
Program an OAI Function Key to a specific function key of the agents DTerm for each desired agent status like step 1 above. After that map different MSF operation codes to the chosen OAI Key Code's as shown in step 2 above. Below an example is given assigning MSF code 128 until 132 to function Key numbers 4 until 8 of extension 2300.

```
AKYD, TN=1, STN=2300, PRI=0, PL TN=1, PL STN=2300, S=0, MWD=0, LN PRE=0, TP=0
 KYN 4, KYI=1, FKY=34 [OAI Key Code 1 ]
AKYD, TN=1, STN=2300, PRI=0, PL TN=1, PL STN=2300, S=0, MWD=0, LN PRE=0, TP=0
 KYN 5, KYI=1, FKY=35 [OAI Key Code 2 ]
AKYD, TN=1, STN=2300, PRI=0, PL TN=1, PL STN=2300, S=0, MWD=0, LN PRE=0, TP=0
 KYN 6, KYI=1, FKY=36 [OAI Key Code 3 ]
AKYD, TN=1, STN=2300, PRI=0, PL TN=1, PL STN=2300, S=0, MWD=0, LN PRE=0, TP=0
 KYN 7, KYI=1, FKY=37 [OAI Key Code 4 ]
AKYD, TN=1, STN=2300, PRI=0, PL TN=1, PL STN=2300, S=0, MWD=0, LN PRE=0, TP=0
 KYN 8, KYI=1, FKY=38 [OAI Key Code 5 ]
```

```
AOKC, KEY-CODE=1, F-KIND=1, C-TONE=1, OP-CODE=128
AOKC, KEY-CODE=2, F-KIND=1, C-TONE=1, OP-CODE=129
AOKC, KEY-CODE=3, F-KIND=1, C-TONE=1, OP-CODE=130
AOKC, KEY-CODE=4, F-KIND=1, C-TONE=1, OP-CODE=131
AOKC, KEY-CODE=5, F-KIND=1, C-TONE=1, OP-CODE=132
```

Note: *To avoid confusion with Operation Codes as mentioned in the PBX Command Manual: please make sure you use the codes mentioned above (128-132)*

4.3.7.3. Agent status switching using one or more access prefix(es)

For single agent status switching access prefix, use the following procedure to configure the PBX:

1. To set up a Mode Set Facility (MSF) code for an Analogue or IP DECT, first use commands ANPD(N) and ASPA(N) to program the OAI prefix.

   ```
   ANPDN, TN=1, 1stDC=*, CI=N, NND=3, BLF=0
   ASPAN, TN=1, ACC=*31, CI=N, SRV=SSCA, SIDA=69, NND=3
   ```

2. Use command AOAC to map an OAI access code to MSF code. In the example below MSF code 128 is assigned to the OAI prefix *31 and OAI access code 130:

   ```
   AOAC, OAI-ACC=130, FKIND=1, OP-CODE=128
   ```

For multiple agent status switching access prefixes use the following procedure to configure the PBX. In the example below MSF codes 128 until 132 are assigned to OAI prefix *31 with respectively OAI access codes 130 until 135:

1. Assign an access prefix for OAI in the number plan as described in step 1 above.

2. Assign a different MSF operation code to each OAI access code.

   ```
   AOAC, OAI-ACC=130, FKIND=1, OP-CODE=128
   AOAC, OAI-ACC=131, FKIND=1, OP-CODE=129
   AOAC, OAI-ACC=132, FKIND=1, OP-CODE=130
   AOAC, OAI-ACC=133, FKIND=1, OP-CODE=131
   AOAC, OAI-ACC=134, FKIND=1, OP-CODE=132
   ```

Note: *To avoid confusion with Operation Codes as mentioned in the PBX Command Manual: please make sure you use the codes mentioned above (128-132)*

4.3.8. Codes for phone based agents

Phone based agents use codes to identify the desired status when a single function key or access code is defined. Entering status information is only applicable for Phone Based Agents. When the steps in 4.2.9 Status switching of phone based agents have been entered it is possible to use this feature. The following codes are defined:

- 0# to logon
- 1# to logoff
- 2# to switch not ready
- 3# to switch ready

- 5# to switch work ready leaving the after call work

In case the required agent status is logged-on, a PIN is requested to identify the agent. For information on how to configure a phone based agent with PIN in BCT see 8.5.10 Manually create a BCT user – the Agent by Phone parts.

In case the required agent status is not ready, a Not Ready Reason (NRR) is requested to identify why the agent is switched not ready. Not Ready Reasons (NRR) are entered in tables in the Business ConneCT Database via BCT Supervisor Dashboard. The information in the **Dial Code** column references the chosen Additional Info digits. After installation, a number of default NRRs are available in the chosen system language. In this example the English NRRs are given with their default dial codes:

Not Ready Reason	Dial Code
Coffee break	1
Lunch	2
Other work	3
Personal affairs	4

For more information on how to configure Not Ready Reasons in BCT, see chapter “Not Ready Reasons” in BCT Administrator Guide.

In case the required agent status is ready, a Call Type (CT) is requested to identify the type or outcome of the handled call. Call Types (CT) are entered in the Business ConneCT database via BCT Supervisor Dashboard. The information in the Dial Code column references the chosen Additional Info digits. After installation, a number of default CTs are available in the chosen system language. In this example the English CTs are given with their default dial codes:

Call Type	Dial Code
Successful	1
Unsuccessful	2

For more information on how to configure Call Types in BCT, see chapter “Call Types” in BCT Administrator Guide.

Note: *A code is always terminated with a # !*

4.3.9. PBX configuration for voicemail

The following programming uses the same group of VMP lines as programmed for the Contact Center programming with VMP lines, so if you already programmed it, you don’t need to do it again. However, you can create another group with different VMP lines if needed. In that case assign different numbers.

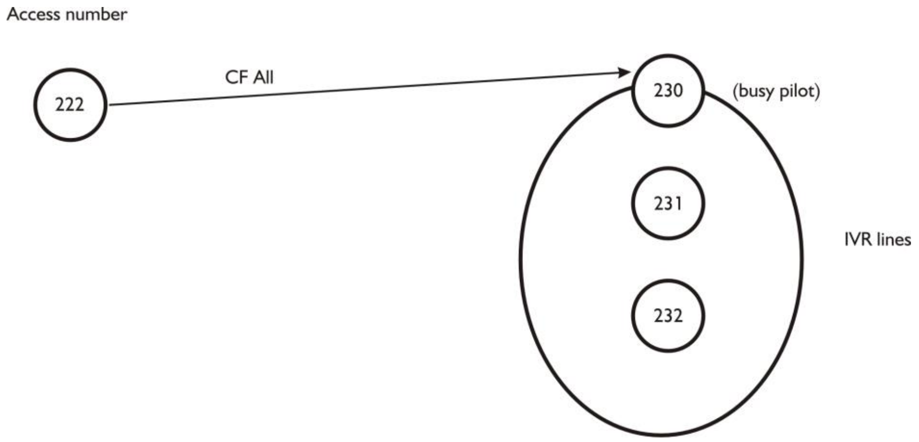


Figure 4-11 Example of configuration for voicemail

Voicemail with VMP IVR lines:

1. Assign 2 IP DTERM for VMP lines using command AISTL and assign TELN numbers using ALGSN:

   AISTL TN=1, IP STN=231, KIND=DTERM IP, TEC=12, RSC=1, SFC=1, LEN=073001 click Set
   AISTL TN=1, IP STN=232, KIND=DTERM IP, TEC=12, RSC=1, SFC=1, LEN=073002 click Set
   AKYD TN=1, STN=231, PRI=0, PL TN=1, PL STN=231, S=0, MWD=0,
   LN PRE=0,TP=0

   In the table that appears:
   KYN= 15, KYI=1, FKY=142, Logout key (in all nodes)
   KYN= 16, KYI=2, KD=0, TN=1, STN=231, RG=7, Myline key (in all nodes)
   AKYD TN=1, STN=232, PRI=0, PL TN=1, PL STN=232, S=0, MWD=0,
   LN PRE=0,TP=0

   In the table that appears:
   KYN= 15, KYI=1, FKY=142, Logout key (in all nodes)
   KYN= 16, KYI=2, KD=0, TN=1, STN=232, RG=7, Myline key (in all nodes)
   ALGSN TYPE=2, UGN=1, TELN=231, FPC=1, TN=1, STN=231
   ALGSN TYPE=2, UGN=1, TELN=232, FPC=1, TN=1, STN=232
   ASDT TN=1, STN=230, LEN=073251, TEC=18, RSC=1, SFC=1
   ALGSN TYPE=2, UGN=1, TELN=230, FPC=1, TN=1, STN=230
   MBST TN=1, STN=230, MB=1
   ASHUN UGN=1, TELN=230, EDIT TELN: 231+232 (press sort all and set)

2. Assign the voicemail access line

   ASDT TN=1, STN=222, LEN=073250, TEC=18, RSC=1, SFC=1
   ALGSN TYPE=2, UGN=1, TELN=222, FPC=1, TN=1, STN=222

3. Set CF all from voicemail access line to the voicemail group pilot number

   ACFS_T TN=1, TELN=222, press Get, select radio buttonTYPE = ‘Call Forwarding’ and SRV = ‘All Calls’. Fill in for CFD 230 then press Set and Exit.

4.3.10. PBX configuration for the special monitored number

To ensure that call handling and call transfer works in all cases, you must configure a special Monitored number. This number is needed for various situations, such as enabling Contact Center agents to transfer calls to other agents, and ending unanswered ISDN calls (by providing a place to park the calls first).

Configure the special Monitored number as follows:

1. Create TELN number:

   ALGNN, UGN=1, TELN=296 (296 is the Special Monitored number)

2. Create Monitored number:

   AMNON A/G=Administrative station, UGN=1, N_MNO=296, N_NMI=8, MFC=0

4.3.11. PBX configuration for FCCS

BCT supports FCCS. With FCCS, multiple PBX systems can be networked together with the look and feel of one system.

The BCT server is connected to the Network Control Node (NCN), which serves as the host for the whole network. The extensions in the Local Control Node (LCN) are monitored by the BCT server as well via the NCN. See Figure 4-7 FCCS network in section 4.3.3 PBX boundaries, options and licenses dedicated for FCCS.

Please refer to the PBX documentation for information on how to make the FCCS connection between the NCN and the LCN(s).

Specific settings needed in the NCN

The NCN contains the configuration as defined in the previous chapter on network level.

All functional programming of Starter Lines, Monitored numbers and UCD groups has to be done in the NCN. Operator, employee and agent clients however can reside everywhere in the network (NCN or LCN)

Specific settings needed in the LCN(s)

The DDI fail conditions in the LCN are forwarded to the same network virtual number (297) as done by the NCN, by means of the command ACFON (Assignment of Call Forwarding Data for NDM).

Note: *BCT requires that all nodes in the FCCS network have the same username and password. You can set the same credentials for all nodes or set the credentials on the NCN.*

4.3.12. SV8500/SV9500 configuration for location diversity

BCT in combination with the SV8500/SV9500 supports Location Diversity. Location Diversity is possible when at least two SV8500/SV9500 systems are interconnected via a FCCS network. BCT is connected to the SV8500/SV9500 via an OAI connection; the system to which BCT is connected is called the Master PBX.

Note for SV9500 Location Diversity: VMP lines and IPDECT phones will not be automatically detected.
So after synchronization, the terminal type of those lines must be manually set to IPDECT.

For VMP lines it means that only after changing the terminal type to IPDECT they will be visible as VMP lines.
When VMP lines needs to be added, a specific sequence must be used in the specified order:

- Create the lines in the PBX
- Sync BCT
- Set the terminal type to IPDECT
- Add them to the VMP group in the PBX
- Sync BCT

Now the new lines will be visible in VMP lines list

Alarms are generated during automatic failover to another SV8500/SV9500 system, or when a failover fails. Other significant events are logged as system status events, see 11.2.1.2 System Status.

For configuration details: see 8.6 Configuring redundant PBX configurations.

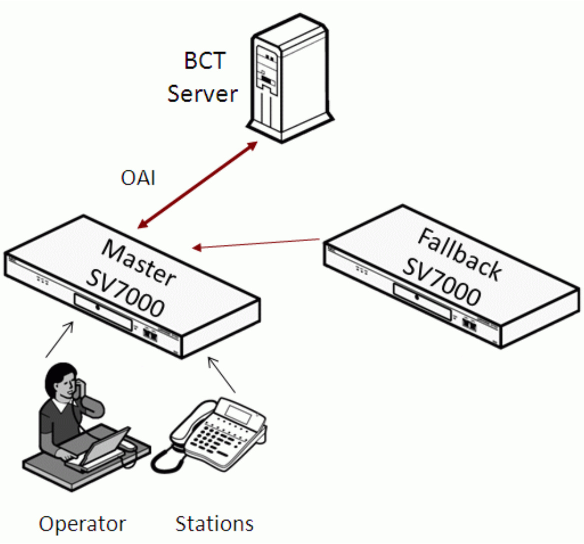


Figure 4-12 Location Diversity System Overview

4.3.13. SV9500 configuration for Geographic Redundancy

BCT in combination with the SV9500 supports Geographic Redundancy. Geographic Redundancy is possible when at least two SV9500 systems are configured to operate in a main / fallback configuration. BCT is connected to the SV9500 via an OAI connection; the system to which BCT is connected is called the Master PBX. When the OAI connection to the master PBX fails, BCT switches over to the other PBX and establishes an OAI connection. Either the main or fallback PBX can be master depending on which node is reachable.

The next configuration must be programmed to enable Geographic Redundancy and have BCT detect at synchronization that Geographic Redundancy is active:

ASYDL	SYS 1 INDEX 1354	bit 0	must be '1'	Geographic Redundancy enabled
ASYDL	SYS 1 INDEX 1199	bit 7	must be '1'	OAI restricted for system in standby mode

Alarms are generated during automatic failover to another SV9500 system, or when a failover fails. Other significant events are logged as system status events, see 11.2.1.2 System Status.

The DRS IP Address (LAN-1) of the backup node must be assigned manually to a configuration file:

- Open the configuration file "PBXConfigurationService.WinService.exe.config" in "C:\Program Files (x86)\Common Files\NEC\Services" with notepad. Look for the section "geoSettings".

- A part of the configuration file looks like:

```
</configuration>
  ...
  <geoSettings>
    <!-- For the fallback node in a Geographic Redundant network add a new key
value entry -->
    <!--  key   = IP Address (LAN-2) of fallback Node     -->
    <!--  value = DRS IP Address (LAN-1) of fallback Node -->
    <!-- Example:                                         -->
    <!-- <add key="192.168.111.52" value="192.168.111.152" /> -->
  </geoSettings></configuration>
```

- The tags "<!--" en "-->" define the line to be comment, so this has to be removed.

- Example of a configured IP Address: LAN-2 is 192.168.111.52 and LAN-1 is 192.168.111.152

```
<geoSettings>
 <add key="192.168.111.52" value="192.168.111.152" />
</geoSettings>
```

For other configuration details: see also 8.6 Configuring redundant PBX configurations.

4.3.14. SV9500 configuration for IP-Centrex

BCT supports IP-Centrex feature of SV9500 (IP Centrex in SV9500 is a function where more than one sub-PBX's can be created within one 'physical' PBX).
The following configuration must be programmed in the SV9500 to enable this feature and let the BCT detect it at the synchronization.

ASYDL	SYS1	INDEX 818	Bit 5 must be 1	Dial Plan to support IP Centrex Functionality is enabled
ASYDL	SYS1	INDEX 871	Bit 5 must be 1	IP Centrex for OAI is enabled

Note – *Upgrading BCT (without IP Centrex) and afterwards synchronizing the PBX while IP Centrex is already enabled in the PBX will move all users to ##**##. Information like voice-mails and greetings may not be accessible anymore as they are stored in a folder structure including the original extension number, however it is not deleted and still present.*

4.3.15. Open number scheme

Supported for SV9500 networks, not for SV8500 networks.
Not supported for any other mixed networks e.g. SV9300/SV9500 networks.
Number conversion to entered numbers for call setup should be activated, see 8.1.11 Dialing Rules.

4.4. UNIVERGE SV8100/SV9100/AspireX/AspireUX configuration

This chapter explains how to set up the PBX type UNIVERGE SV8100/SV9100, AspireX/AspireUX and SV9100-TAPI for BCT. The main configuration items concern operators, voicemail and the Contact Center.

Make sure that you have the following PBX-licenses available in the PBX:

- License code 0123: OAI Activation; (not required for SV9100-TAPI)
- License code 0112: 3rd party CTI Client; (required for SV9100-TAPI only)
- License code 5111: IP Terminal (SIP-SLT/3rd Party); required if IVR is used.

It is possible to configure in the BCT System Settings (**Connection** tab) and/or License Manager (**File > Load New License String** menu option) where to obtain the BCT licenses, if they reside in the PBX. The License Manager (re)loads the licenses automatically at least once a day, so that when licenses in the PBX are upgraded, BCT will automatically use them.

The PBX is programmed with PC Pro using Easy Edit Pages. The starting point is a PBX with default settings. When the PBX is programmed according this chapter, the Configuration Wizard can be used to configure BCT.

For the PC Pro SV8100 GE and the PC Pro AspireX/AspireUX without Easy Edit pages the programming should be done with Program Commands in System Data. SV8100 and SV9100 have a different version of PCPro and Easy Edit. The most extended version is shown as figure.

1. Set the Push flag mode for OAI with terminal programming:

   Program 99-03-26 to 1 (PSH ON).

2. Set Retrieve Line After Transfer to Not Holding:

   Program 20-02-04 to 0 / Not Active. The default value of the AspireX/AspireUX is not correct.

3. To prevent analogue trunk lockout, busy tone detection should be used:

   Enable detection in program 14-02-09, 14-02-12 and 14-02-18
   Program 80-04-06 and 80-04-08 for tone 2 (busy tone for trunk) to 4 (150 ms).

4.4.1. Connection to a PBX

The following figure shows the preferred network configuration. The IP addresses shown will be used in the configuration description.

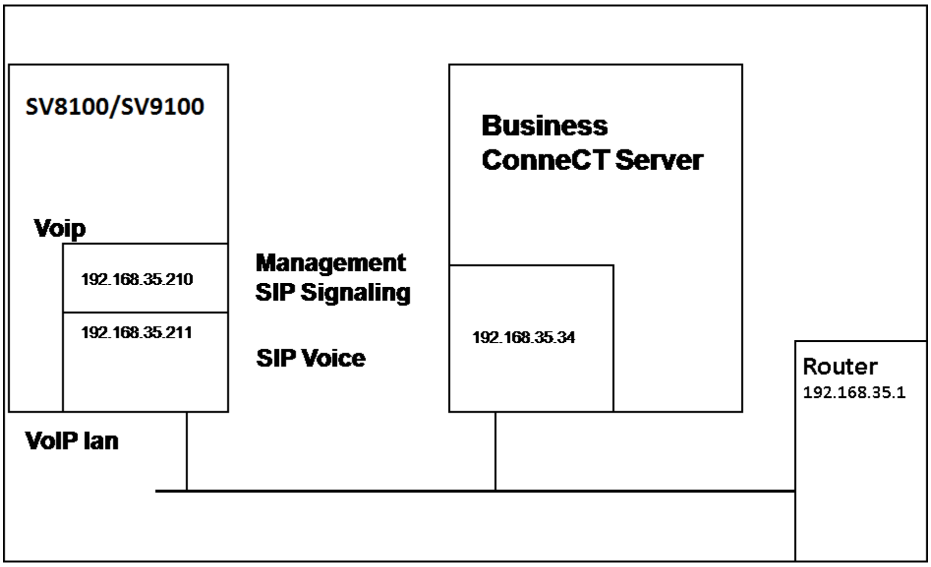


Figure 4-13 PBX connection to the BCT Server

In this example, the PBX is equipped with a CCPU in slot 1 and a 128 channel VoIP board. The Router can be used to connect terminals from another segment.

The IPLA IP Address 192.168.35.210 is used by the BCT server for synchronization, OAI/TAPI management and SIP connection.

4.4.2. Scripts and examples

You can use the scripts on the BCT product DVD (PBX Scripts folder) as a basis for projecting a standalone PBX system. The scripts contain a standard operator, voicemail, and starter entries. In this manual, the projecting of the PBX follows the examples of the figures in the following sections. The examples can be used when the PBX system is in the state when it has only initial system data.

You must change the station numbers, hardware addresses etc. to the ones you require.

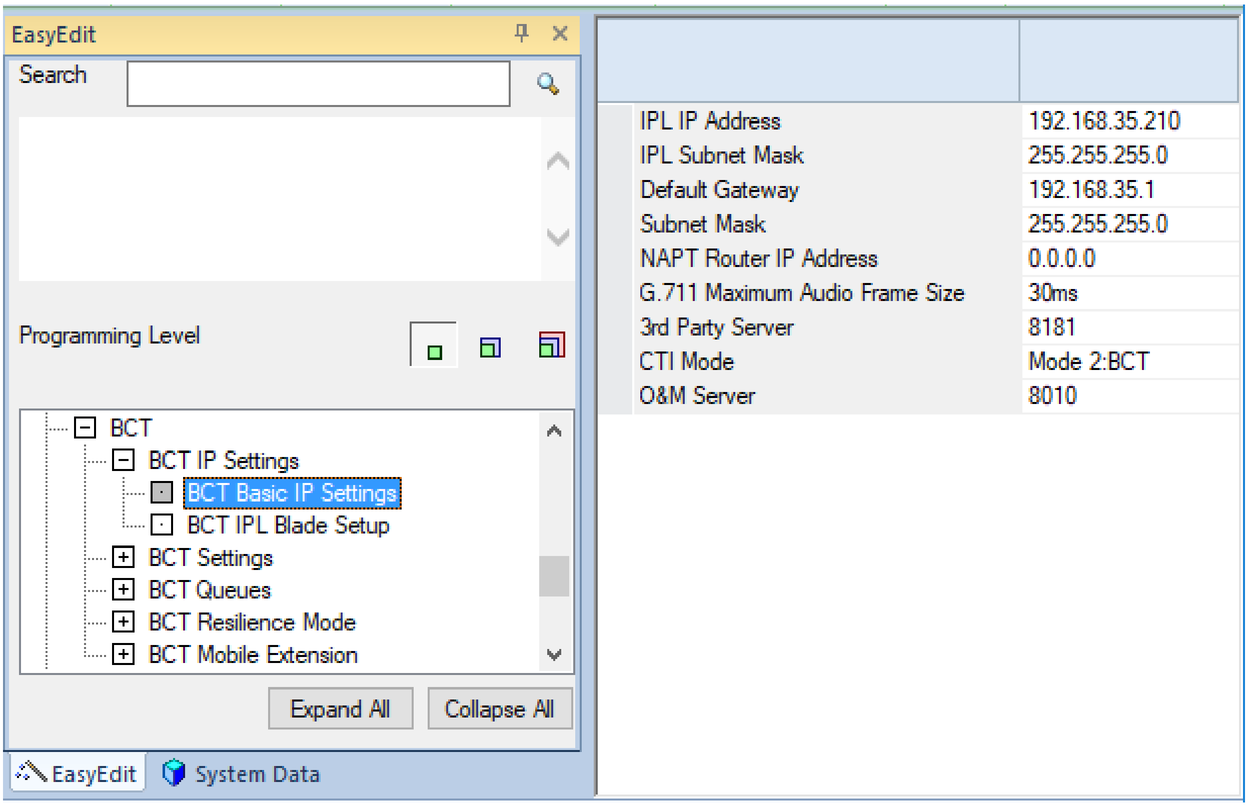
Note: *not all PC Pro versions support scripts.*

4.4.3. PBX programming using Easy Edit Pages

Using PC Pro, open the wizard tab and navigate to **Applications, BCT**.

BCT IP Settings, BCT BASIC IP Settings

Specify a valid IPLA IP address, routing and IPLA Subnet Mask to allow the SIP signaling and OAI or TAPI.



IPL IP Address	192.168.35.210
IPL Subnet Mask	255.255.255.0
Default Gateway	192.168.35.1
Subnet Mask	255.255.255.0
NAPT Router IP Address	0.0.0.0
G.711 Maximum Audio Frame Size	30ms
3rd Party Server	8181
CTI Mode	Mode 2:BCT
O&M Server	8010

Figure 4-14 BCT Basic IP Settings

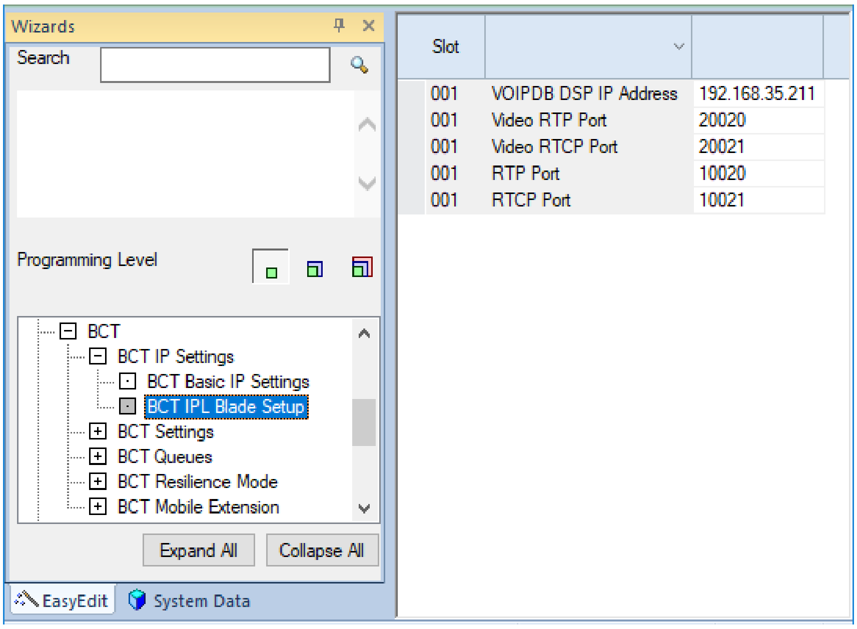
Important: *Set G.7.11 Maximum Audio Frame Size the same as the VMP line Setting payload (default 30 msec).*

Program Command	Item	Setting
10-12-09	IPLA IP Address	192.168.35.210
10-12-02	Subnet Mask	255.255.255.0
10-12-03	Default Gateway	192.168.35.1
10-12-10	IPLA Subnet Mask	255.255.255.0
84-19-01	G.711 Maximum Audio Frame Size	30ms
10-20-01	CTI Server / 3rd Party Server	8181
20-23-09 10-26-05 (SV8100)	CTI Mode	Mode 2:BCT (SV9100-TAPI) Mode 1 (SV8100)
10-20-11	O&M Server	8010

Note: *CTI Mode will be automatically set to 2 for SV9100-TAPI.*

BCT IP Settings, BCT IPLA Blade Setup

Assign IP addresses to your DSP resources.



Slot		
001	VOIPDB DSP IP Address	192.168.35.211
001	Video RTP Port	20020
001	Video RTCP Port	20021
001	RTP Port	10020
001	RTCP Port	10021

Figure 4-15 BCT IPLA Blade setup

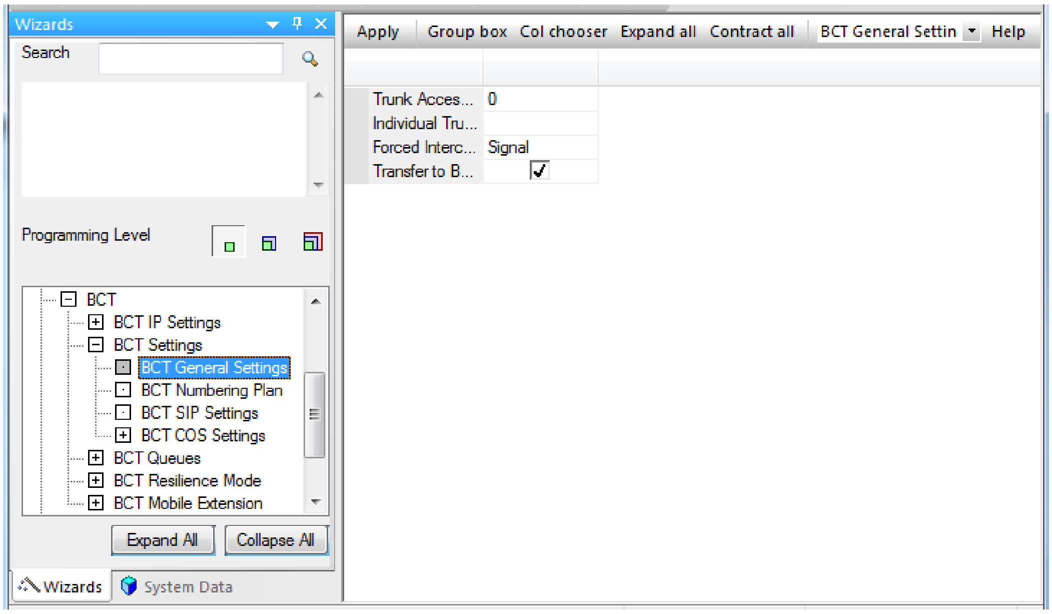
Program Command	Item	Setting
84-26-01 VoIP Gateway 1	IP Address	192.168.35.211

Note: *Please note that changes to IP addressing within the PBX require a reboot.*

BCT Settings, BCT General Settings

Define the trunk access code. The 'Forced intercom ringing' has to be set to “Signal”.

It is possible to Enable Transfer to Busy Extension for Camp On busy functionality. Note that this is a system wide option. For Camp On via BCT for standard SIP and IPDect, 99-03-51 should be set via Terminal programming. Both settings require SV8100 R4 or higher.



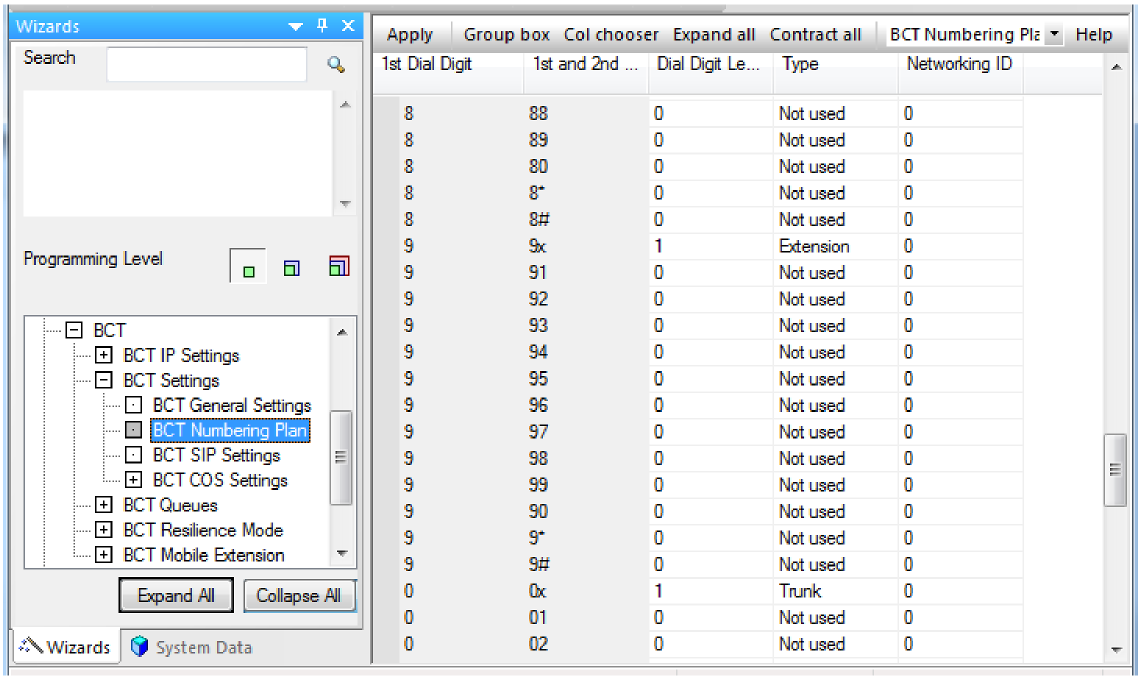
Trunk Acces...	0
Individual Tru...	
Forced Interc...	Signal
Transfer to B...	☑

Figure 4-16 BCT Settings, BCT General Settings

Program Command	Item	Setting
11-01-01 0x	Digit	1
11-01-01 0x	Type	Trunk
11-09-01	Trunk Access Code	0
20-02-12	Forced Intercom Ringing	Signal
24-02-01	Transfer to Busy Extension	Enable for Camp On Busy (R4 and up)
99-03-51	Camp On for st.SIP and IPDect	1 (via Terminal programming) (R4 and up)

BCT Numbering Plan

Use this page to define which numbers can be dialed. The trunk access code needs to be reflected in the system numbering plan. Use this screen when considering what number range to use for Extension Numbering, including Virtual extensions for Queue positions, Pilot Groups for Routing Points and SIP Extensions for VMP lines. It is possible to define a digit to reach the Operator internally by setting it as a 1 digit extension. This single digit can then be used to define the internal Queue's pilot number.



1st Dial Digit	1st and 2nd ...	Dial Digit Le...	Type	Networking ID
8	88	0	Not used	0
8	89	0	Not used	0
8	80	0	Not used	0
8	8*	0	Not used	0
8	8#	0	Not used	0
9	9x	1	Extension	0
9	91	0	Not used	0
9	92	0	Not used	0
9	93	0	Not used	0
9	94	0	Not used	0
9	95	0	Not used	0
9	96	0	Not used	0
9	97	0	Not used	0
9	98	0	Not used	0
9	99	0	Not used	0
9	90	0	Not used	0
9	9*	0	Not used	0
9	9#	0	Not used	0
0	0x	1	Trunk	0
0	01	0	Not used	0
0	02	0	Not used	0

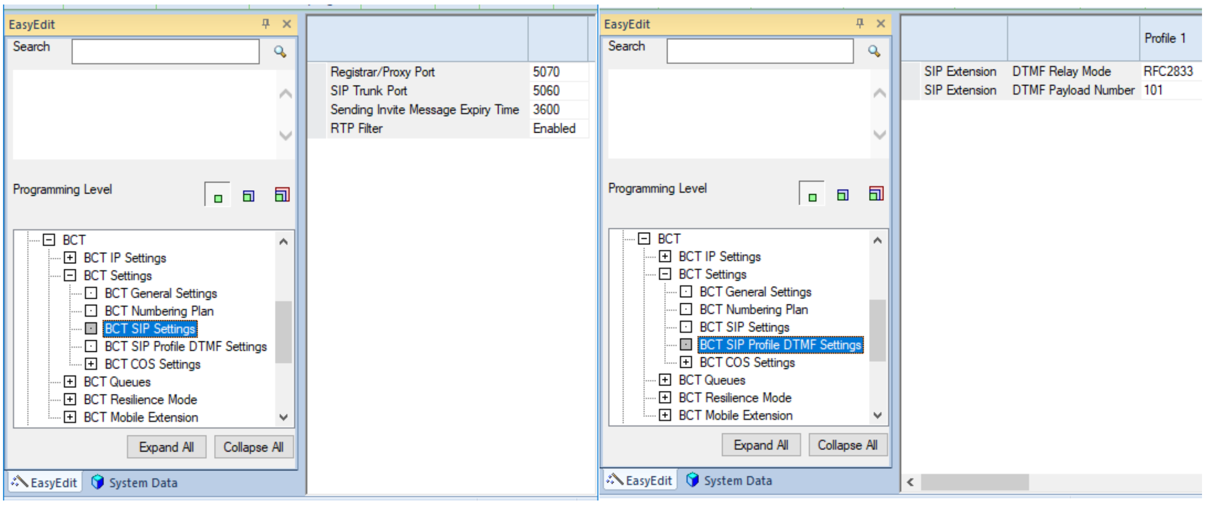
Figure 4-17 BCT Numbering Plan

Program Command	Item	Setting
11-01-01 9x	Digit	1
11-01-01 9x	Type	Extension

BCT SIP Settings and BCT SIP Profile DTMF Settings

Use this page to define some options in preparation for creating the SIP Extensions that will be used as VMP lines, if applicable.

- SIP Peer to Peer = Off
- Peer to Peer = On
- RTP Forwarding Mode = Off
- DT700 Peer to Peer = On
- Registrar/Proxy Port = 5070 (this is also the BCT default)
- SIP Trunk Port = 5060 (only required to change if Registrar/Proxy port is changed to 5060)
- Sending Invite Message Expiry Time = 3600
- DTMF Relay Mode = RFC2833, DTMF Payload Number = 101
- RTP Filter = On



Registrar/Proxy Port	5070
SIP Trunk Port	5060
Sending Invite Message Expiry Time	3600
RTP Filter	Enabled

		Profile 1
SIP Extension	DTMF Relay Mode	RFC2833
SIP Extension	DTMF Payload Number	101

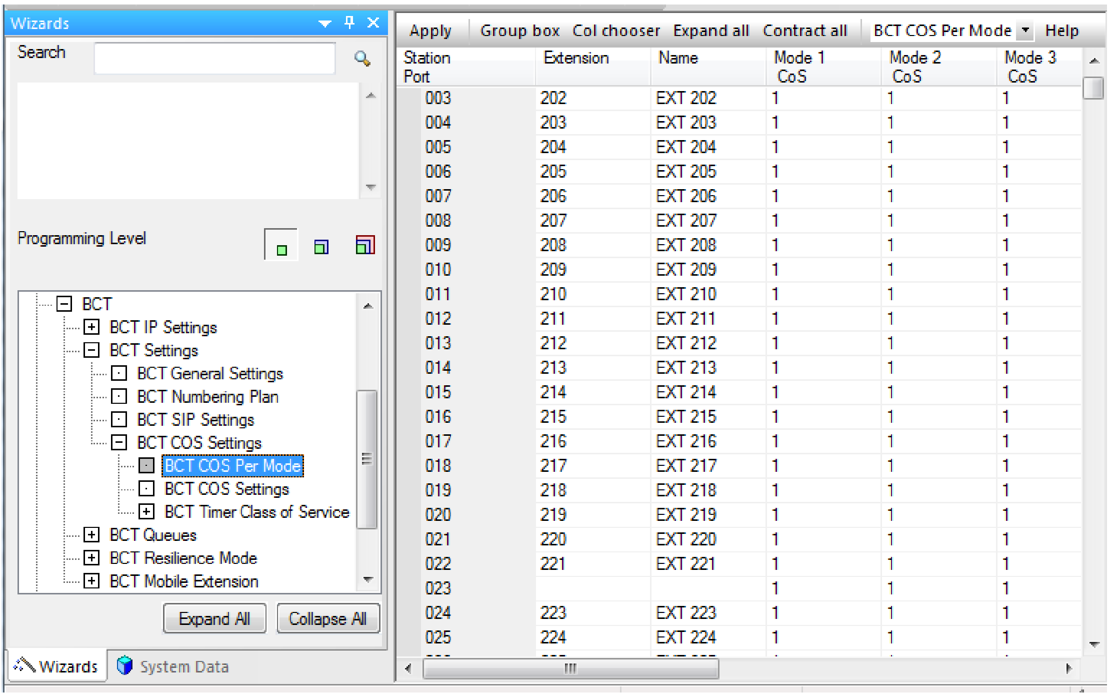
Figure 4-18 BCT SIP Settings and BCT SIP Profile DTMF Settings

The 10-26 commands are only for the SV8100.
SV9100: use 15-05-50 to set peer to peer mode, use 84-34-01/02 to set DTMF for active profile.

Program Command	Item	Setting
10-26-01	Peer to Peer Mode	On
10-26-02	RTP Forwarding Mode	Off
10-26-03	SIP Peer to Peer	Off
10-26-04	DT700 Peer to Peer	On
84-19-31	DTMF Payload Number	101
84-19-32	DTMF Relay Mode	RFC2833
84-19-49	RTP Filter	On
84-14-06	SIP Trunk Port	5060
84-20-01	Registrar/Proxy Port	5070
84-20-06	Sending Invite Message Expiry Time	3600

BCT COS Per Mode

When anything other than COS 1 is used for your extension return to this section after configuring the BCT Queues. Put your extensions into the relevant COS.



Station Port	Extension	Name	Mode 1 CoS	Mode 2 CoS	Mode 3 CoS
003	202	EXT 202	1	1	1
004	203	EXT 203	1	1	1
005	204	EXT 204	1	1	1
006	205	EXT 205	1	1	1
007	206	EXT 206	1	1	1
008	207	EXT 207	1	1	1
009	208	EXT 208	1	1	1
010	209	EXT 209	1	1	1
011	210	EXT 210	1	1	1
012	211	EXT 211	1	1	1
013	212	EXT 212	1	1	1
014	213	EXT 213	1	1	1
015	214	EXT 214	1	1	1
016	215	EXT 215	1	1	1
017	216	EXT 216	1	1	1
018	217	EXT 217	1	1	1
019	218	EXT 218	1	1	1
020	219	EXT 219	1	1	1
021	220	EXT 220	1	1	1
022	221	EXT 221	1	1	1
023			1	1	1
024	223	EXT 223	1	1	1
025	224	EXT 224	1	1	1

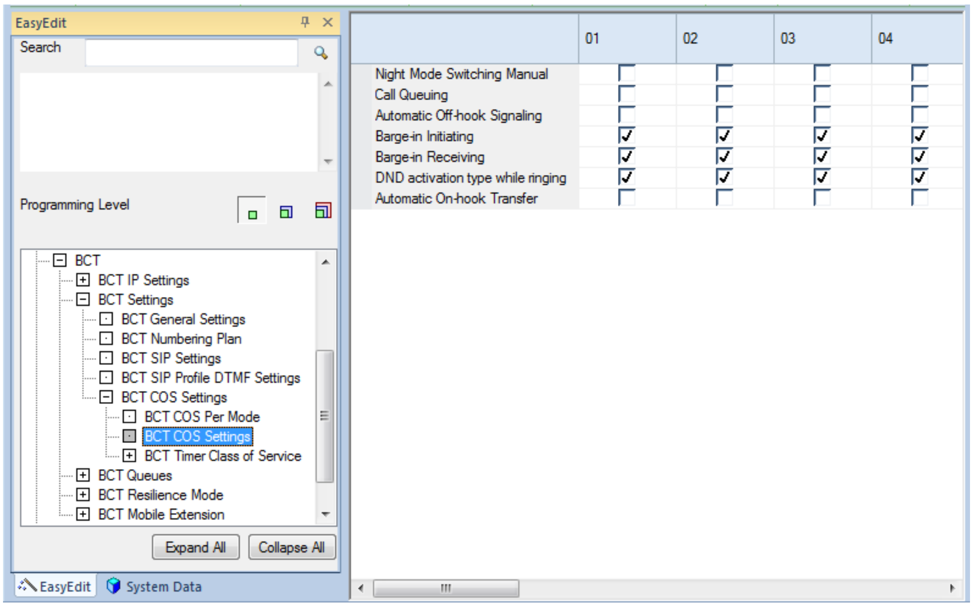
Figure 4-19 BCT COS per Mode

Program Command	Item	Setting
20-06-01	Night Mode	1

BCT COS Settings

The following options should be set against the relevant COS:

- Call Queuing = OFF
- Automatic Off-hook Signaling = OFF
- Barge-in Initiate = ON
- Barge-in Receive = ON
- DND activation type while ringing = ON
- Automatic On-hook Transfer = OFF



	01	02	03	04
Night Mode Switching Manual	□	□	□	□
Call Queuing	□	□	□	□
Automatic Off-hook Signaling	□	□	□	□
Barge-in Initiating	☑	☑	☑	☑
Barge-in Receiving	☑	☑	☑	☑
DND activation type while ringing	☑	☑	☑	☑
Automatic On-hook Transfer	□	□	□	□

Figure 4-20 BCT COS Settings

Program Command	Item	Setting
20-09-07	Call Queuing	Off
20-13-06	Automatic Off-hook Signaling	Off
20-13-15	Barge-in Initiating	On
20-13-16	Barge-in Receive	On
20-09-13	DND activation type while ringing	On
20-11-11	Automatic On-hook Transfer	Off

BCT requires Queues and VMP lines to handle calls for the Operator, Contact Center and Voicemail.

For Operator calls and IVR-less Contact Center calls department groups are used that consist of Virtual extensions as group members. The group pilot is used as Routing Point.

For Voicemail calls and Contact Center IVR calls a department group is used that consists of SIP VMP lines as group members. The group pilot is used as the Voicemail access number.

Note: *For Contact Center only systems, there should be at least 1 Routing Point configured in Supervisor Dashboard, for parking a call during transferring the call to an agent.*

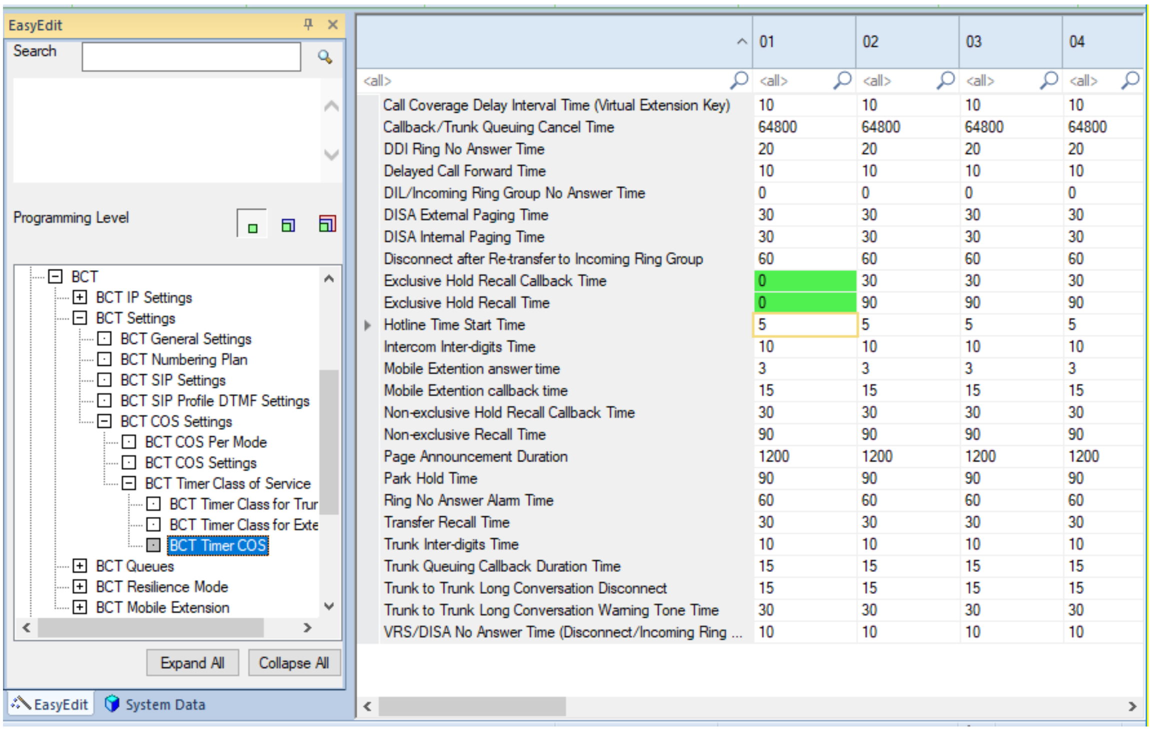
Finally, two department groups will be used in case of System Fallback when the BCT server is down or cannot be reached. The department group for System Fallback for the operator consists of the operator extensions as group members. The department group for System Fallback for the Contact Center consist of the agent extensions as group members.

BCT Settings, BCT COS Settings, BCT Timer COS

Hold Recall time for BCT extensions has to be set 0.

The Normal (Non-exclusive) Hold Recall and Exclusive Hold Recall Timers should be disabled for BCT users.

BCT Extensions should be placed in a Timer Class for (20-29) and the recall for that timer class disabled (0 entered) for Non-exclusive Hold Recall (item 11), Exclusive Hold Recall (item 12).



	01	02	03	04
<all>	<all>	<all>	<all>	<all>
Call Coverage Delay Interval Time (Virtual Extension Key)	10	10	10	10
Callback/Trunk Queuing Cancel Time	64800	64800	64800	64800
DDI Ring No Answer Time	20	20	20	20
Delayed Call Forward Time	10	10	10	10
DIL/Incoming Ring Group No Answer Time	0	0	0	0
DISA External Paging Time	30	30	30	30
DISA Internal Paging Time	30	30	30	30
Disconnect after Re-transfer to Incoming Ring Group	60	60	60	60
Exclusive Hold Recall Callback Time	0	30	30	30
Exclusive Hold Recall Time	0	90	90	90
Hotline Time Start Time	5	5	5	5
Intercom Inter-digits Time	10	10	10	10
Mobile Extention answer time	3	3	3	3
Mobile Extention callback time	15	15	15	15
Non-exclusive Hold Recall Callback Time	30	30	30	30
Non-exclusive Recall Time	90	90	90	90
Page Announcement Duration	1200	1200	1200	1200
Park Hold Time	90	90	90	90
Ring No Answer Alarm Time	60	60	60	60
Transfer Recall Time	30	30	30	30
Trunk Inter-digits Time	10	10	10	10
Trunk Queuing Callback Duration Time	15	15	15	15
Trunk to Trunk Long Conversation Disconnect	15	15	15	15
Trunk to Trunk Long Conversation Warning Tone Time	30	30	30	30
VRS/DISA No Answer Time (Disconnect/Incoming Ring ...	10	10	10	10

Figure 4-21 BCT Settings, BCT COS Settings, BCT Timer COS

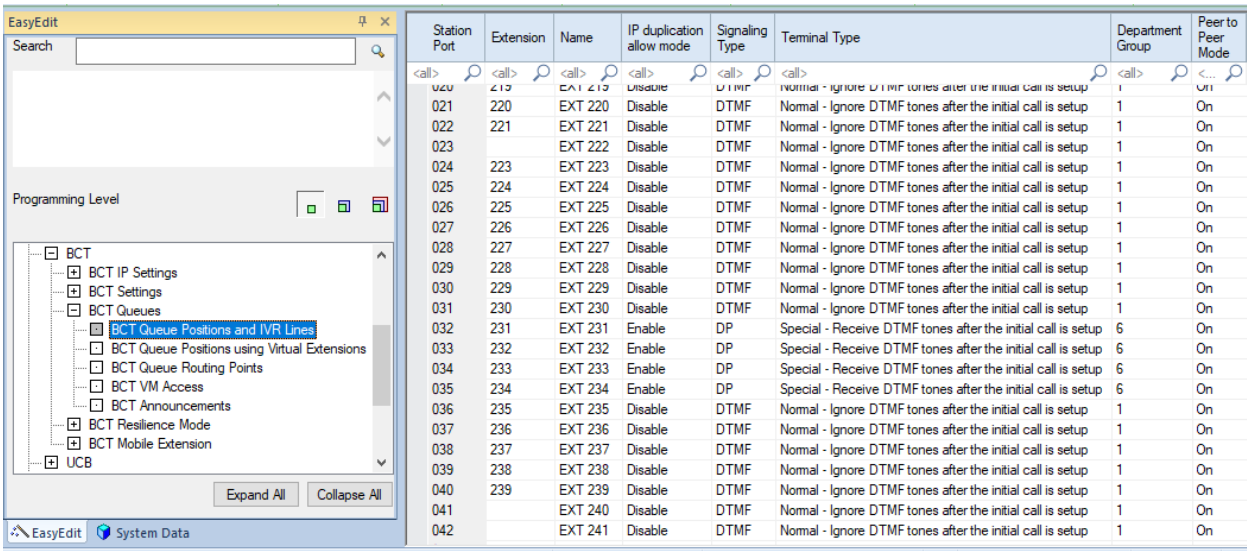
Program Command	Item	Setting
20-29-01	Timer Class for extensions	1 for used Modes and BCT extensions
20-31-11	Non-exclusive Hold Recall Time	0 (do not recall) for timer 1
20-31-12	Exclusive Hold Recall Time	0 (do not recall) for timer 1

BCT Queue Positions and VMP Lines

Use this page when configuring SIP VMP Lines. The number of group members defines the maximum Queue size. For example: (with 4 VMP lines):

Group Name	Group Number	Group Pilot (Voicemail access)	Group Members
VMaccess	6	222	231-234

- **Extension** = a valid Extension number.
- **Name** = a meaningful name to denote what the extension is
- **IP Duplication Allowed mode =** enabled to make more than one phone on the same IP address possible. (SV8100: IP Duplication Allowed Group = Group1)
- **Signaling Type** = **DP** (to reduce the system resource usage)
- **Terminal Type** = **Special** (to allow DTMF tones to be received after the initial call is setup)
- **Department Group** = the number of the department group the extension is a member of.



Station Port	Extension	Name	IP duplication allow mode	Signaling Type	Terminal Type	Department Group	Peer to Peer Mode
<all>	<all>	<all>	<all>	<all>	<all>	<all>	<...
020	219	EXT 219	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
021	220	EXT 220	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
022	221	EXT 221	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
023		EXT 222	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
024	223	EXT 223	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
025	224	EXT 224	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
026	225	EXT 225	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
027	226	EXT 226	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
028	227	EXT 227	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
029	228	EXT 228	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
030	229	EXT 229	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
031	230	EXT 230	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
032	231	EXT 231	Enable	DP	Special - Receive DTMF tones after the initial call is setup	6	On
033	232	EXT 232	Enable	DP	Special - Receive DTMF tones after the initial call is setup	6	On
034	233	EXT 233	Enable	DP	Special - Receive DTMF tones after the initial call is setup	6	On
035	234	EXT 234	Enable	DP	Special - Receive DTMF tones after the initial call is setup	6	On
036	235	EXT 235	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
037	236	EXT 236	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
038	237	EXT 237	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
039	238	EXT 238	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
040	239	EXT 239	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
041		EXT 240	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On
042		EXT 241	Disable	DTMF	Normal - Ignore DTMF tones after the initial call is setup	1	On

Figure 4-22 BCT Queue positions and VMP Lines

Remove 222, 240, 241, 242, 243, 244, 293, 294, 295, 297 and 298 from the extension list.

IMPORTANT:

1. The IP Duplication Groups should be programmed before use, never afterwards

2. Make sure that only the required VMP lines belong to the IP Duplication Group

3. Reduce resource usage with program 15-03-01 on Signaling Type DP for VMP lines

4. Department group properties are programmed together with the BCT Queue Routing Point.

When no Easy Edit: Make the unregistered SIP lines 231-234 visible via Programming Unregistered and IP Phone List...

Program Command	Item	Setting
11-07-01 Department Group 6	Pilot	222
16-02-01 Extension 231-234	Department Group	6
15-03-01 Extension 231-234	Signaling Type	DP
15-03-03 Extension 231-234	Terminal Type	Special – Receive DTMF tones after the initial call is setup
15-05-18 Extension 231-234	IP Duplication Allowed Mode	Enable
11-02	Remove from extension list	

Note: *When 15-03-03 is not possible with PC Pro, use terminal programming.*

SV9100 specific:

15-05-50 Peer to Peer Mode: Disable for all VMP lines and SIP extensions

BCT Queuing Positions Using Virtual Extensions

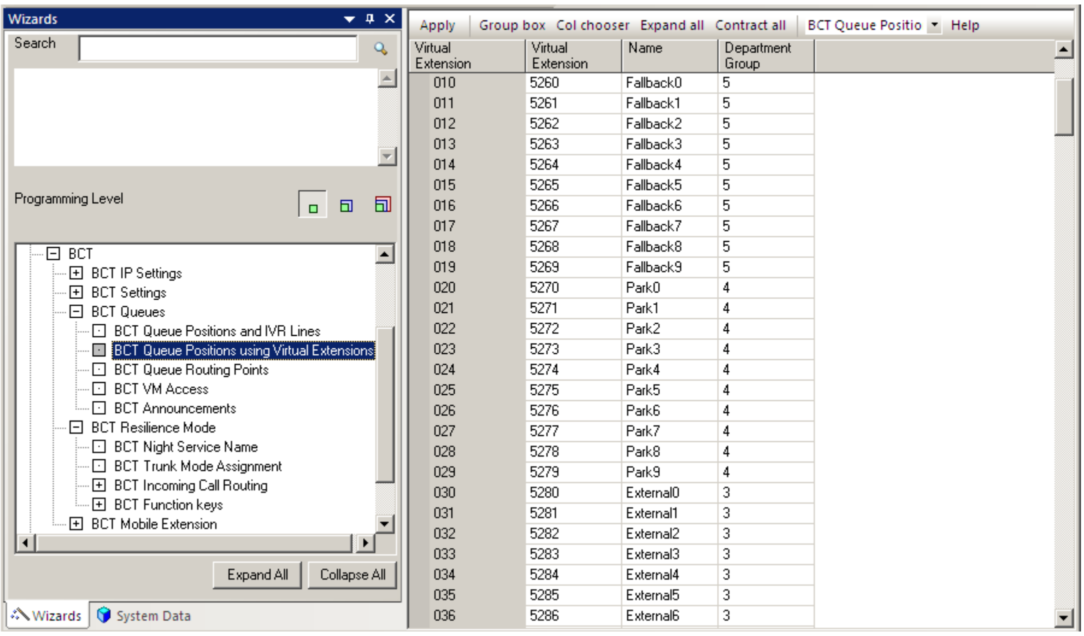
Use this page when configuring Virtual extension Queue Positions. The number of Group Members defines the Maximum Queue Size.

Virtual Queue Positions are used by BCT 4.1 and later.

For example:

Group Name (queue name)	Group Number	Group Pilot (routing points)	Group Members (queue positions)
Internal	2	9	5290-5299
External	3	295	5280-5289
Park	4	294	5270-5279
Fallback	5	293	5260-5269

- **Extension** = a valid Extension number to be a Queue Position
- **Name** = a meaningful name to denote what the extension is
- **Department Group** = the number of the department group\ Routing Point the extension is a member of.



Virtual Extension	Virtual Extension	Name	Department Group
010	5260	Fallback0	5
011	5261	Fallback1	5
012	5262	Fallback2	5
013	5263	Fallback3	5
014	5264	Fallback4	5
015	5265	Fallback5	5
016	5266	Fallback6	5
017	5267	Fallback7	5
018	5268	Fallback8	5
019	5269	Fallback9	5
020	5270	Park0	4
021	5271	Park1	4
022	5272	Park2	4
023	5273	Park3	4
024	5274	Park4	4
025	5275	Park5	4
026	5276	Park6	4
027	5277	Park7	4
028	5278	Park8	4
029	5279	Park9	4
030	5280	External0	3
031	5281	External1	3
032	5282	External2	3
033	5283	External3	3
034	5284	External4	3
035	5285	External5	3
036	5286	External6	3

Figure 4-23 BCT Queue Positions Using Virtual Extensions

Program Command	Item	Setting
11-04-01 Port 001 - 049	Virtual Extension	5260 - 5299
15-01-01 ICM Ext 5290 - 5299	Name	Internal0 – Internal9
15-01-01 ICM Ext 5280 - 5289	Name	External0 – External9
15-01-01 ICM Ext 5270 - 5279	Name	Park0 – Park9
15-01-01 ICM Ext 5260 - 5269	Name	Fallback0 – Fallback9

16-02-01 ICM Ext 5290 - 5299	Department Group	2
16-02-01 ICM Ext 5280 - 5289	Department Group	3
16-02-01 ICM Ext 5270 - 5279	Department Group	4
16-02-01 ICM Ext 5260 - 5269	Department Group	5

BCT also supports the use of IVR-less Contact Center Routing Points, the configuration of which follows the same rules as the other Routing Points, where by the positions are created as Virtual extensions and added as members to a pilot group.

An example of IVR-less Contact Center Routing Points (**not in PCPro screen figures**):

Group Name (queue name)	**Group Number**	**Group Pilot (routing points)**	**Group Members (queue positions)**
Services	8	240	5300-5309
Sales	9	241	5310-5319
Support	10	242	5320-5329

In this table, three Routing Points are created for the IVR-less Contact Center: service, sales and support. This way the Contact Center can distinguish between incoming calls and the agent can answer the phone appropriately.

***Note**: When the BCT system needs many Starter Lines it is not necessary to create a Routing Point for each of the starter lines separately (note that the number of pilots is limited); create a Virtual extension for each Starter Line and assign permanent immediate forwarding on each of the VE's to a single Routing Point (large enough to hold a lot of queue positions).*
(Use 24-09-01/02/03/06 to assign the forwarding relations).

Program Command	**Item**	**Setting**
11-07-01 Department Group 8	Pilot	240
11-07-01 Department Group 9	Pilot	241
11-07-01 Department Group 10	Pilot	242
16-01-01 Department Group 8	Name	Services
16-01-01 Department Group 9	Name	Sales
16-01-01 Department Group 10	Name	Support
16-01-02 Department Group 8 – 10	Calling Cycle	Circular Routing
16-01-04 Department Group 8 – 10	Hunting Mode	Circular
16-01-07 Department Group 8 – 10	Call Recall Restriction	Enabled (Non-recall)
16-01-09 Department Group 8 – 10	Call No Answer Time	0
11-04-01 Port 050 - 079	Virtual Extension	5300 - 5329
16-02-01 ICM Ext 5300 - 5309	Department Group	8
16-02-01 ICM Ext 5310 - 5319	Department Group	9
16-02-01 ICM Ext 5320 - 5329	Department Group	10

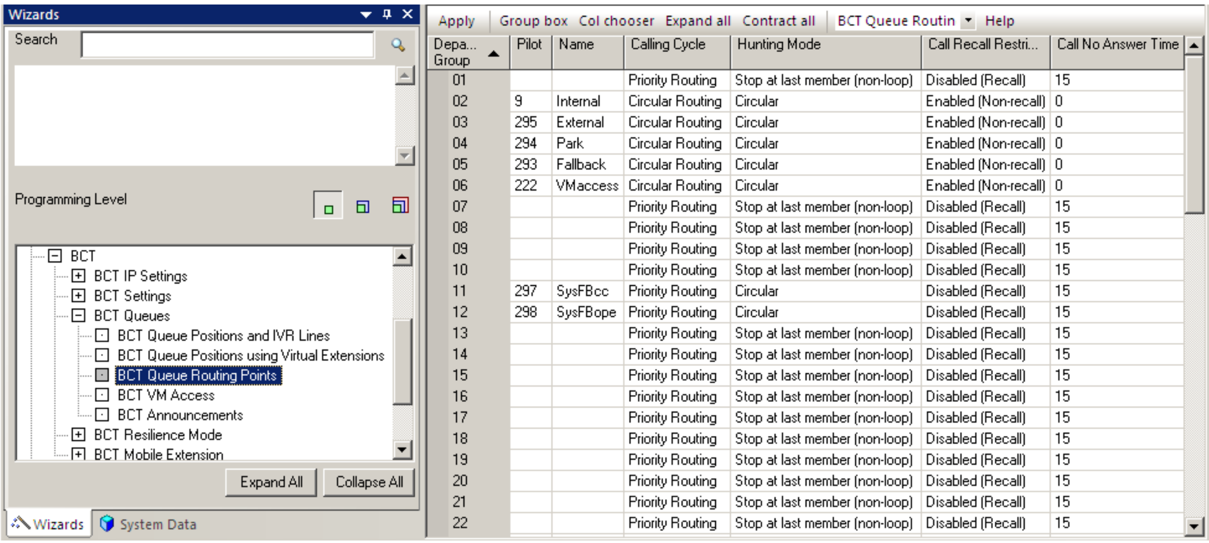
Note: *To use the System Call Park functionality for operators (also called Pickup Park) a separate set of Routing points need to be configured. Every System Call Park position requires a separate Routing point.*

The configuration of the Routing points follows the same rules as the Routing Points for the other operator queues. However, because only one Pickup and Park position is used for every Routing point, only one Virtual number needs to be configured as member in the Department group. The created Department groups will now be seen as routing points by BCT and can be used for System Call Park. For BCT configuration for System Call Park see 8.3.10 Create System Call Park configuration*.*

BCT Queue Routing Points

Use this page to define the group pilots for the Queue positions, the IVR group (voicemail access) and the System Fallback groups. For Queues and the IVR group use the following settings:

- **Pilot** = assign a valid number for the Pilot Group Number
- **Name** = used to identify the Group
- **Calling Cycle** = Circular Routing
- Hunting Mode = Circular
- Call Recall Restriction = Enabled
- Call No Answer Time = 0



Depa... Group	Pilot	Name	Calling Cycle	Hunting Mode	Call Recall Restri...	Call No Answer Time
01			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
02	9	Internal	Circular Routing	Circular	Enabled (Non-recall)	0
03	295	External	Circular Routing	Circular	Enabled (Non-recall)	0
04	294	Park	Circular Routing	Circular	Enabled (Non-recall)	0
05	293	Fallback	Circular Routing	Circular	Enabled (Non-recall)	0
06	222	VMaccess	Circular Routing	Circular	Enabled (Non-recall)	0
07			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
08			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
09			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
10			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
11	297	SysFBcc	Priority Routing	Circular	Disabled (Recall)	15
12	298	SysFBope	Priority Routing	Circular	Disabled (Recall)	15
13			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
14			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
15			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
16			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
17			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
18			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
19			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
20			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
21			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15
22			Priority Routing	Stop at last member (non-loop)	Disabled (Recall)	15

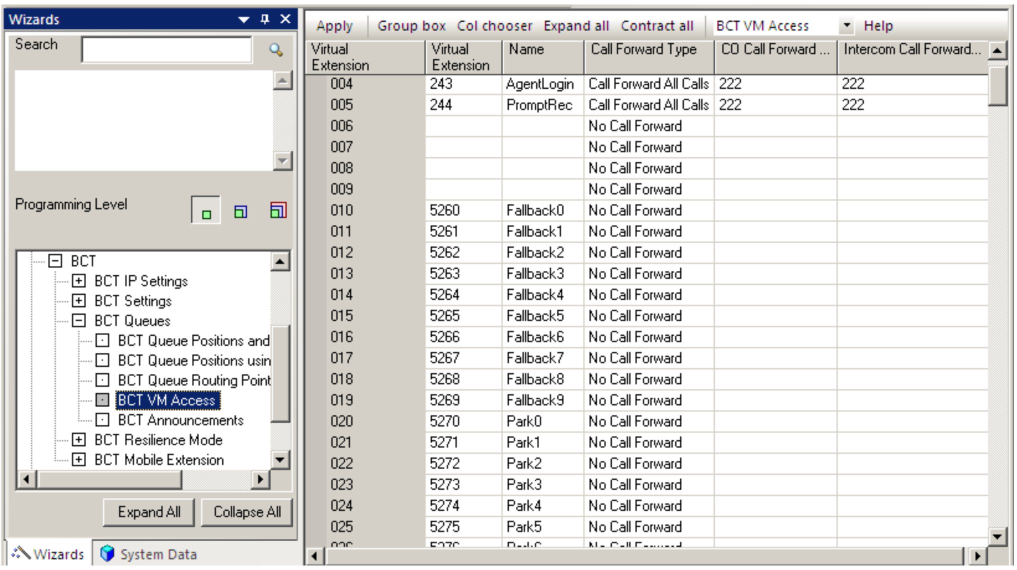
Figure 4-24 BCT Queue Routing Points

Program Command	Item	Setting
11-07-01 Department Group 2	Pilot	9
11-07-01 Department Group 3	Pilot	295
11-07-01 Department Group 4	Pilot	294
11-07-01 Department Group 5	Pilot	293
11-07-01 Department Group 6	Pilot	222
16-01-01 Department Group 2	Name	Internal
16-01-01 Department Group 3	Name	External
16-01-01 Department Group 4	Name	Park
16-01-01 Department Group 5	Name	Fallback
16-01-01 Department Group 6	Name	VMaccess
16-01-02 Department Group 2 – 6	Calling Cycle	Circular Routing
16-01-04 Department Group 2 – 6	Hunting Mode	Circular
16-01-07 Department Group 2 – 6	Call Recall Restriction	Enabled (Non-recall)
16-01-09 Department Group 2 – 6	Call No Answer Time	0

BCT VM Access

This page is used to defined the Contact Center access to IVR features, for example Auto Attendant, phone based login, and Prompt recording. These Virtual extensions are nominated within BCT to define their roles. In contrast, the Voicemail access should be the group pilot of the IVR group and not one of the Virtual extensions.

Call Forward All Calls is set to point to the IVR Pilot Group (voicemail access) for both trunk and intercom calls.



Virtual Extension	Virtual Extension	Name	Call Forward Type	CO Call Forward ...	Intercom Call Forward...
004	243	AgentLogin	Call Forward All Calls	222	222
005	244	PromptRec	Call Forward All Calls	222	222
006			No Call Forward		
007			No Call Forward		
008			No Call Forward		
009			No Call Forward		
010	5260	Fallback0	No Call Forward		
011	5261	Fallback1	No Call Forward		
012	5262	Fallback2	No Call Forward		
013	5263	Fallback3	No Call Forward		
014	5264	Fallback4	No Call Forward		
015	5265	Fallback5	No Call Forward		
016	5266	Fallback6	No Call Forward		
017	5267	Fallback7	No Call Forward		
018	5268	Fallback8	No Call Forward		
019	5269	Fallback9	No Call Forward		
020	5270	Park0	No Call Forward		
021	5271	Park1	No Call Forward		
022	5272	Park2	No Call Forward		
023	5273	Park3	No Call Forward		
024	5274	Park4	No Call Forward		
025	5275	Park5	No Call Forward		

Figure 4-25 BCT VM Access

***Note:** BCT Announcements are not used by the standard BCT.*

When the Configuration Wizard is used a Virtual extension for “Logon”, "Prompt recording" and “AgentGroup” is required.

Program Command	Item	Setting
11-04-01 Port 001 - 005	Virtual Extension	243-244
15-01-01 ICM Extension 243	Name	AgentLogin
15-01-01 ICM Extension 244	Name	PromptRec
24-09-01 ICM Extension 240 - 244	Call Forward Type	Call Forward All Calls
24-09-02 ICM Extension 240 - 244	CO Call Forward Destination for Both Ring, All Calls and No Answer	222
24-09-03 ICM Extension 240 - 244	Intercom Call Forward Destination for Both Ring, All Calls and No Answer	222

AspireX/AspireUX: check chapter 4.4.7 Presence setting to external destinations (AspireX/AspireUX only) if program 24-06 or program 24-09 needs to be used.

BCT DDI Routing table

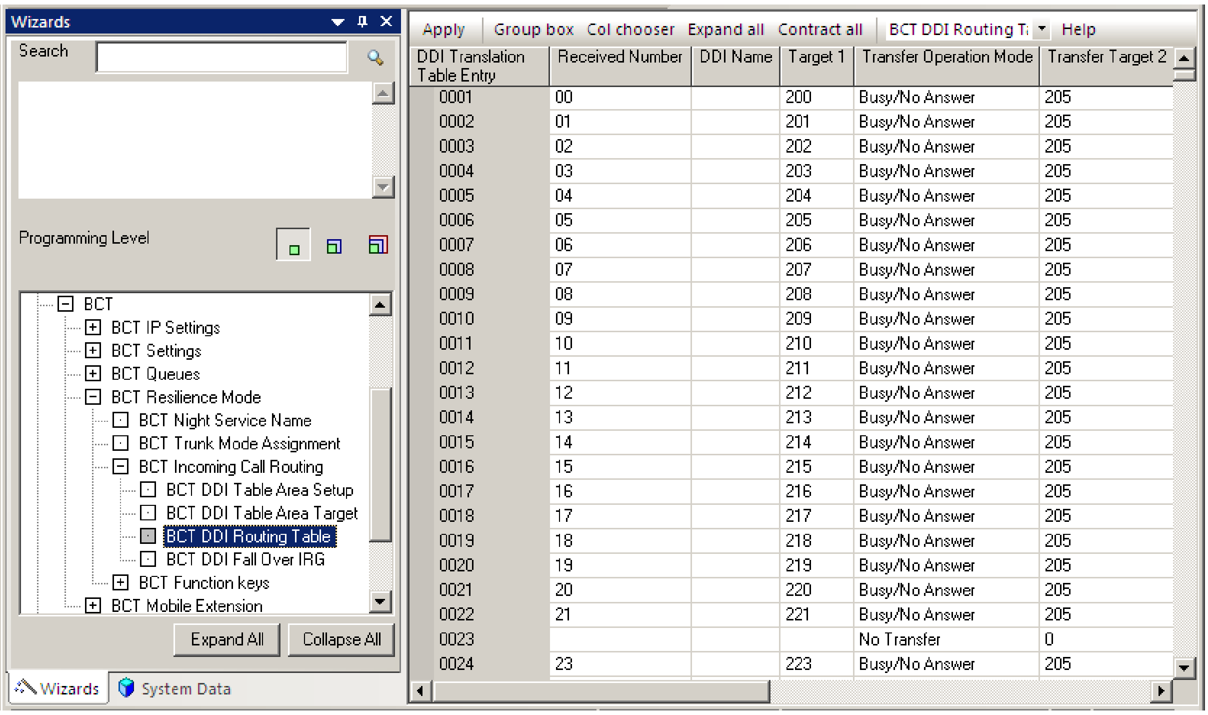
Use this page to transfer DDI fail actions (external calls to Busy, Not Answering, DND or vacant extensions) to the Fallback Queue of the operator. This table defines what extension to call when a number is received over a trunk. Beside normal extensions, also Contact Center access, external operator Queue and other extensions used by BCT should be added to the Translation table when they need to be called over a trunk. In a default PBX during Normal mode the DDI table Area 01 is used with a Starting Address 1 and Ending Address 200.

To define DDI fail actions for calls to Busy, Not Answering and DND extensions, every extension in the DDI translation Table should be changed to the following settings:

- Transfer Operation Mode = Busy/No Answer
- Transfer Target 2 = 205 (2 stands for type Department group, 05 stands for Department group number, which is the FallBack Queue)

To define DDI fail actions for calls to vacant extensions the Ending DDI Translation table entry (200) should be change to the following setting

- Received number = “@@”
- DDI Name = useful name (e.g. Fallback)
- Target 1 = (not filled in)
- Transfer Operation Mode = Busy/No Answer
- Transfer Target 2 = 205



DDI Translation Table Entry	Received Number	DDI Name	Target 1	Transfer Operation Mode	Transfer Target 2
0001	00		200	Busy/No Answer	205
0002	01		201	Busy/No Answer	205
0003	02		202	Busy/No Answer	205
0004	03		203	Busy/No Answer	205
0005	04		204	Busy/No Answer	205
0006	05		205	Busy/No Answer	205
0007	06		206	Busy/No Answer	205
0008	07		207	Busy/No Answer	205
0009	08		208	Busy/No Answer	205
0010	09		209	Busy/No Answer	205
0011	10		210	Busy/No Answer	205
0012	11		211	Busy/No Answer	205
0013	12		212	Busy/No Answer	205
0014	13		213	Busy/No Answer	205
0015	14		214	Busy/No Answer	205
0016	15		215	Busy/No Answer	205
0017	16		216	Busy/No Answer	205
0018	17		217	Busy/No Answer	205
0019	18		218	Busy/No Answer	205
0020	19		219	Busy/No Answer	205
0021	20		220	Busy/No Answer	205
0022	21		221	Busy/No Answer	205
0023				No Transfer	0
0024	23		223	Busy/No Answer	205

Figure 4-26 BCT DDI Routing Table

Program Command	Item	Setting
22-11-04 Entry 1 - 99	Transfer Operation Mode	Busy/No Answer
22-11-05 Entry 1 – 99	Transfer Target 2	205

22-11-01 Entry 200	Received Number	@@
22-11-02 Entry 200	Target 1	
22-11-03 Entry 200	DDI Name	Fallback
22-11-04 Entry 200	Transfer Operation Mode	Busy/No Answer
22-11-05 Entry 200	Transfer Target 2	205

System Fallback via Resilience Mode

When the BCT server is down or cannot be reached, the PBX should go to System Fallback. External calls to the operator (also unsuccessful external calls to Busy/NoAnswer extensions) and to the contact Center should be rerouted to System Fallback group for operator and Contact Center. To program System Fallback the Resilience mode of the PBX is used.

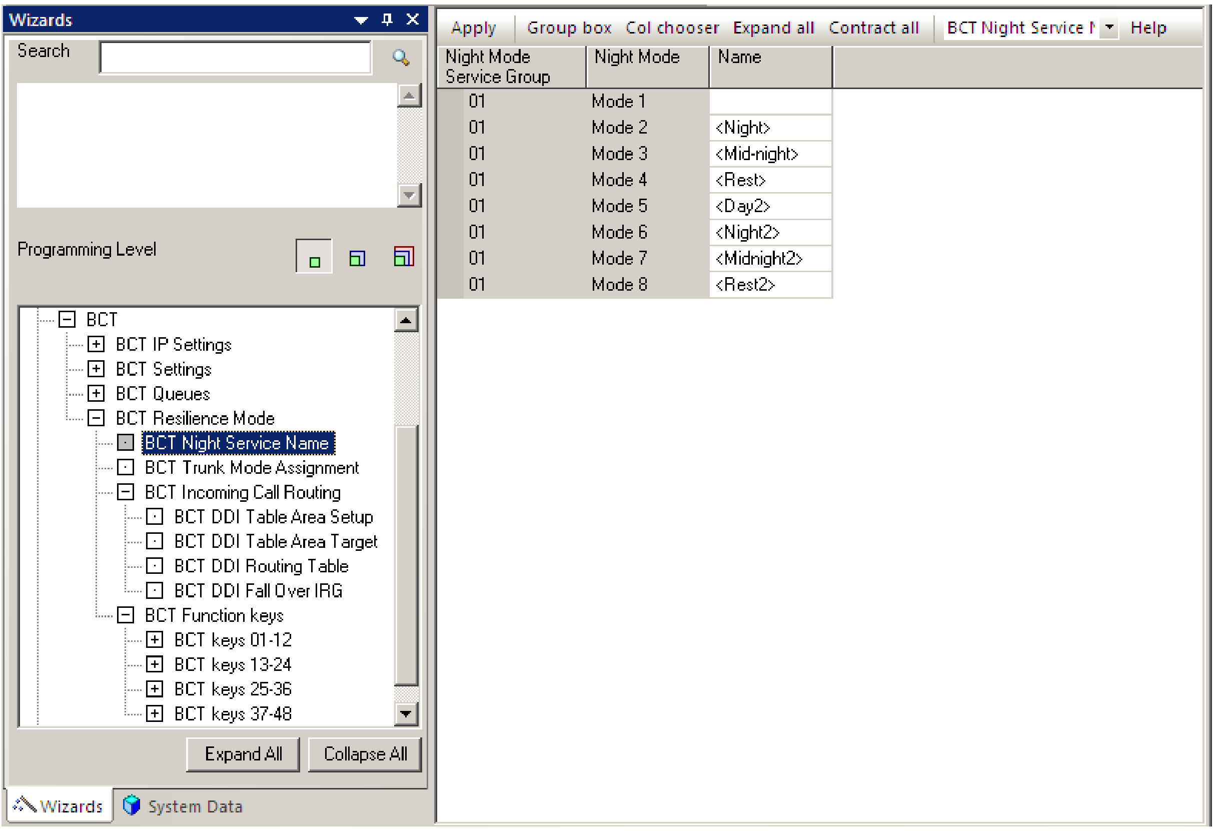
When a System Fallback occurs then the resilience mode can be activated with a Function Key (FK).

A DDI trunk selects a different table area in Resilience mode. The DDI routing table selects the system Fallback group with real extensions as group members.

E.g. the operator extensions and agent extensions can be assigned to the correct department group for System Fallback

Group Name	Group Number	Group Pilot	Group Members
SysFBcc	11	297	210-211
SysFBope	12	298	200

Use Night Mode 4 <Rest> as BCT system Fallback.

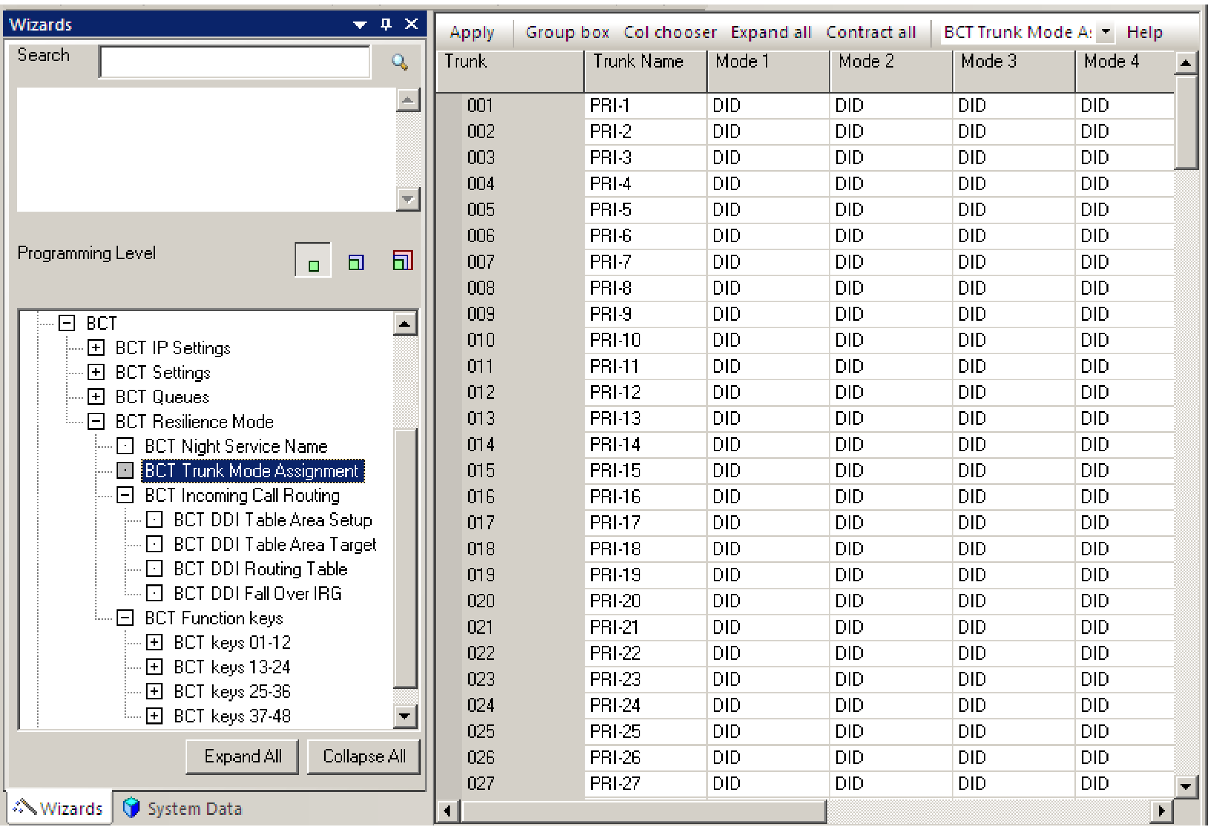


Night Mode Service Group	Night Mode	Name
01	Mode 1	
01	Mode 2	<Night>
01	Mode 3	<Mid-night>
01	Mode 4	<Rest>
01	Mode 5	<Day2>
01	Mode 6	<Night2>
01	Mode 7	<Midnight2>
01	Mode 8	<Rest2>

Figure 4-27 BCT Night Service Name

Program Command	Item	Setting
12-07-01	Night Mode	

Your trunk should be programmed in Mode 4 too:

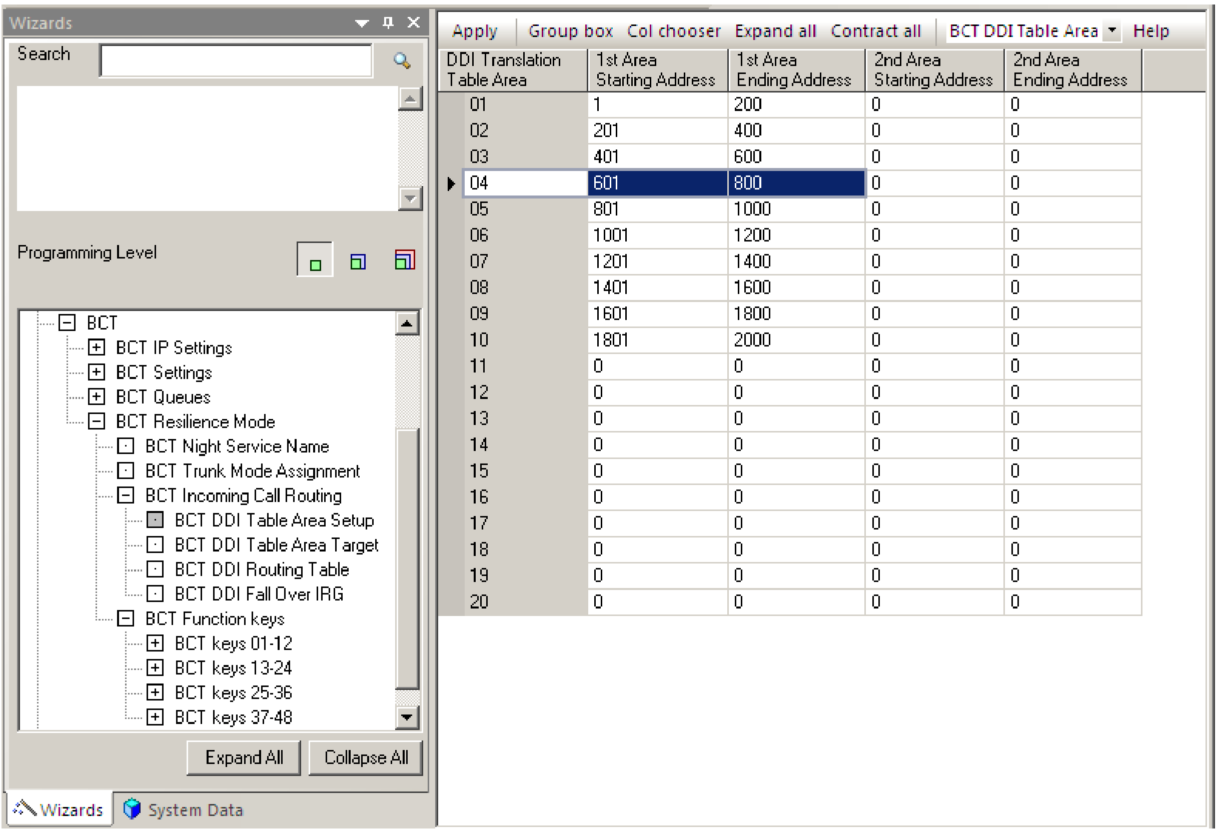


Trunk	Trunk Name	Mode 1	Mode 2	Mode 3	Mode 4
001	PRI-1	DID	DID	DID	DID
002	PRI-2	DID	DID	DID	DID
003	PRI-3	DID	DID	DID	DID
004	PRI-4	DID	DID	DID	DID
005	PRI-5	DID	DID	DID	DID
006	PRI-6	DID	DID	DID	DID
007	PRI-7	DID	DID	DID	DID
008	PRI-8	DID	DID	DID	DID
009	PRI-9	DID	DID	DID	DID
010	PRI-10	DID	DID	DID	DID
011	PRI-11	DID	DID	DID	DID
012	PRI-12	DID	DID	DID	DID
013	PRI-13	DID	DID	DID	DID
014	PRI-14	DID	DID	DID	DID
015	PRI-15	DID	DID	DID	DID
016	PRI-16	DID	DID	DID	DID
017	PRI-17	DID	DID	DID	DID
018	PRI-18	DID	DID	DID	DID
019	PRI-19	DID	DID	DID	DID
020	PRI-20	DID	DID	DID	DID
021	PRI-21	DID	DID	DID	DID
022	PRI-22	DID	DID	DID	DID
023	PRI-23	DID	DID	DID	DID
024	PRI-24	DID	DID	DID	DID
025	PRI-25	DID	DID	DID	DID
026	PRI-26	DID	DID	DID	DID
027	PRI-27	DID	DID	DID	DID

Figure 4-28 BCT Trunk Mode Assignment

Program Command	Item	Setting
22-02-01	Mode 1- 4	DID

DDI Translation Table 04 uses by default Starting Address 601 to 800

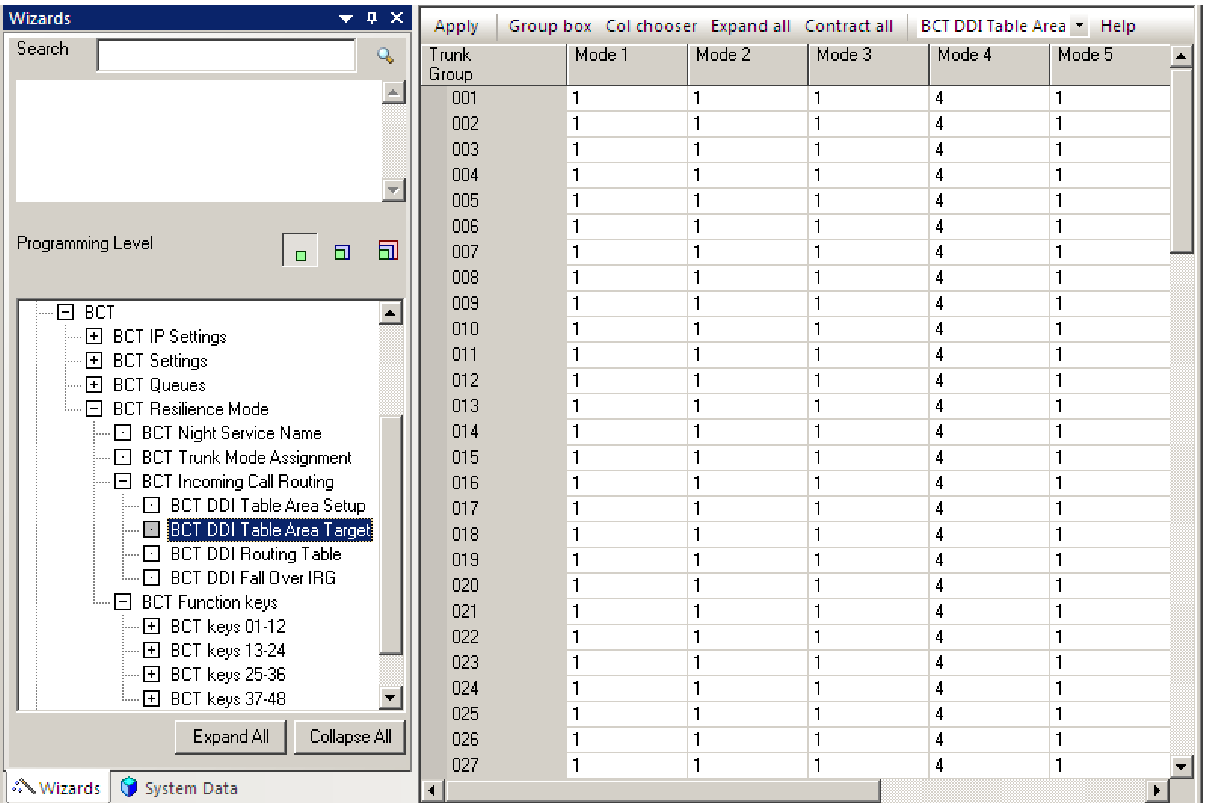


DDI Translation Table Area	1st Area Starting Address	1st Area Ending Address	2nd Area Starting Address	2nd Area Ending Address
01	1	200	0	0
02	201	400	0	0
03	401	600	0	0
04	601	800	0	0
05	801	1000	0	0
06	1001	1200	0	0
07	1201	1400	0	0
08	1401	1600	0	0
09	1601	1800	0	0
10	1801	2000	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0

Figure 4-29 BCT DDI Table Area Setup

Program Command	**Item**	**Setting**
22-10-01	DDI Translation Table Area Setup	

Select for every used trunk group table area 4 in Night Mode 4.



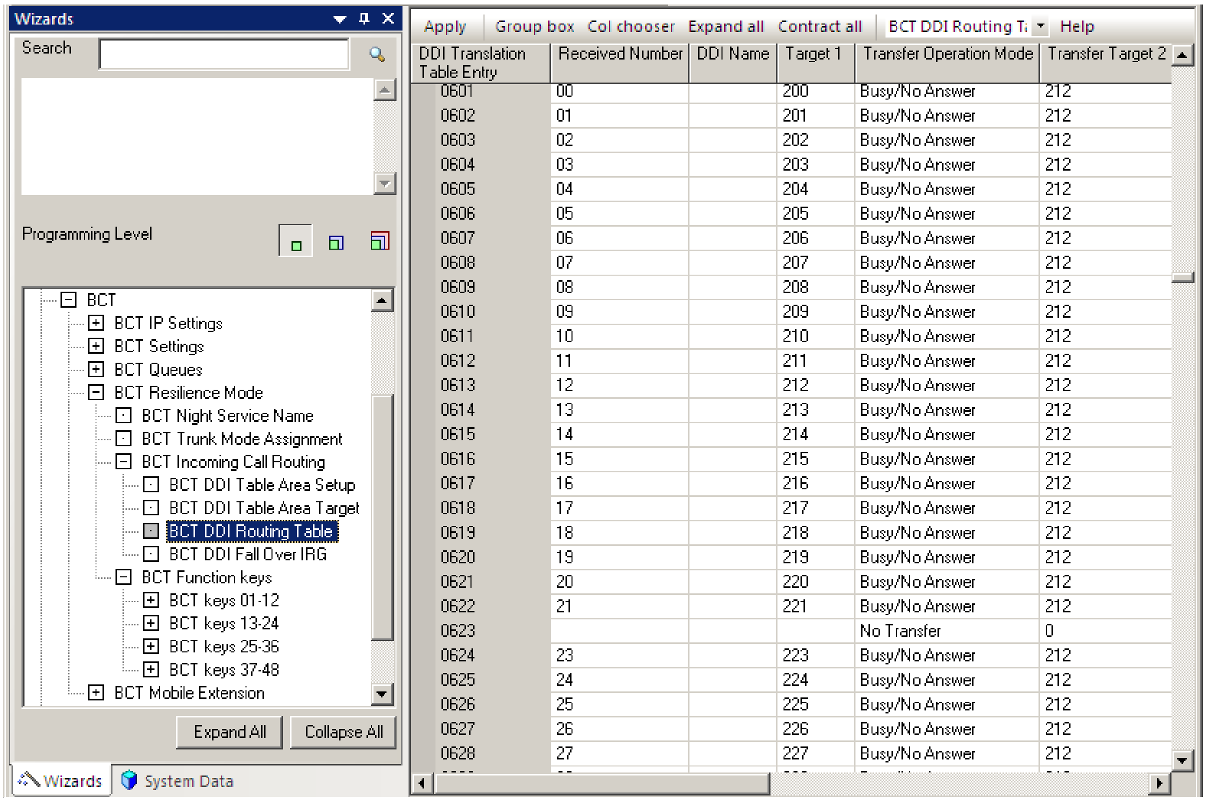
Trunk Group	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
001	1	1	1	4	1
002	1	1	1	4	1
003	1	1	1	4	1
004	1	1	1	4	1
005	1	1	1	4	1
006	1	1	1	4	1
007	1	1	1	4	1
008	1	1	1	4	1
009	1	1	1	4	1
010	1	1	1	4	1
011	1	1	1	4	1
012	1	1	1	4	1
013	1	1	1	4	1
014	1	1	1	4	1
015	1	1	1	4	1
016	1	1	1	4	1
017	1	1	1	4	1
018	1	1	1	4	1
019	1	1	1	4	1
020	1	1	1	4	1
021	1	1	1	4	1
022	1	1	1	4	1
023	1	1	1	4	1
024	1	1	1	4	1
025	1	1	1	4	1
026	1	1	1	4	1
027	1	1	1	4	1

Figure 4-30 BCT DDI Table Area Target

Program Command	Item	Setting
22-13-01	Mode 4	4

In a default PBX the Translation Table Entry 601 - 800 can be programmed in the same way as for Normal Mode 1 (table entry 001-200), but now the System Fallback for operators is selected instead of the BCT fallback Queue. The digits received for the external operator Queue should have the pilot of the department group System Fallback for operators (e.g. 298) as Target 1.

For DDI fail- vacant numbers Translation table entry 800 should be filled in with “@@” as Received number and the pilot of the department group System Fallback for operators (e.g. 298) as Target 1.



DDI Translation Table Entry	Received Number	DDI Name	Target 1	Transfer Operation Mode	Transfer Target 2
0601	00		200	Busy/No Answer	212
0602	01		201	Busy/No Answer	212
0603	02		202	Busy/No Answer	212
0604	03		203	Busy/No Answer	212
0605	04		204	Busy/No Answer	212
0606	05		205	Busy/No Answer	212
0607	06		206	Busy/No Answer	212
0608	07		207	Busy/No Answer	212
0609	08		208	Busy/No Answer	212
0610	09		209	Busy/No Answer	212
0611	10		210	Busy/No Answer	212
0612	11		211	Busy/No Answer	212
0613	12		212	Busy/No Answer	212
0614	13		213	Busy/No Answer	212
0615	14		214	Busy/No Answer	212
0616	15		215	Busy/No Answer	212
0617	16		216	Busy/No Answer	212
0618	17		217	Busy/No Answer	212
0619	18		218	Busy/No Answer	212
0620	19		219	Busy/No Answer	212
0621	20		220	Busy/No Answer	212
0622	21		221	Busy/No Answer	212
0623				No Transfer	0
0624	23		223	Busy/No Answer	212
0625	24		224	Busy/No Answer	212
0626	25		225	Busy/No Answer	212
0627	26		226	Busy/No Answer	212
0628	27		227	Busy/No Answer	212

Figure 4-31 BCT DDI Routing Table

Program Command	Item	Setting
22-11-04 Entry 600 – 699	Transfer Operation Mode	Busy No Answer
22-11-05 Entry 600 - 699	Transfer Target 2	212
22-11-01 Entry 800	Received Number	@@
22-11-02 Entry 800	Target 1	298
22-11-03 Entry 800	DDI Name	SysFBope

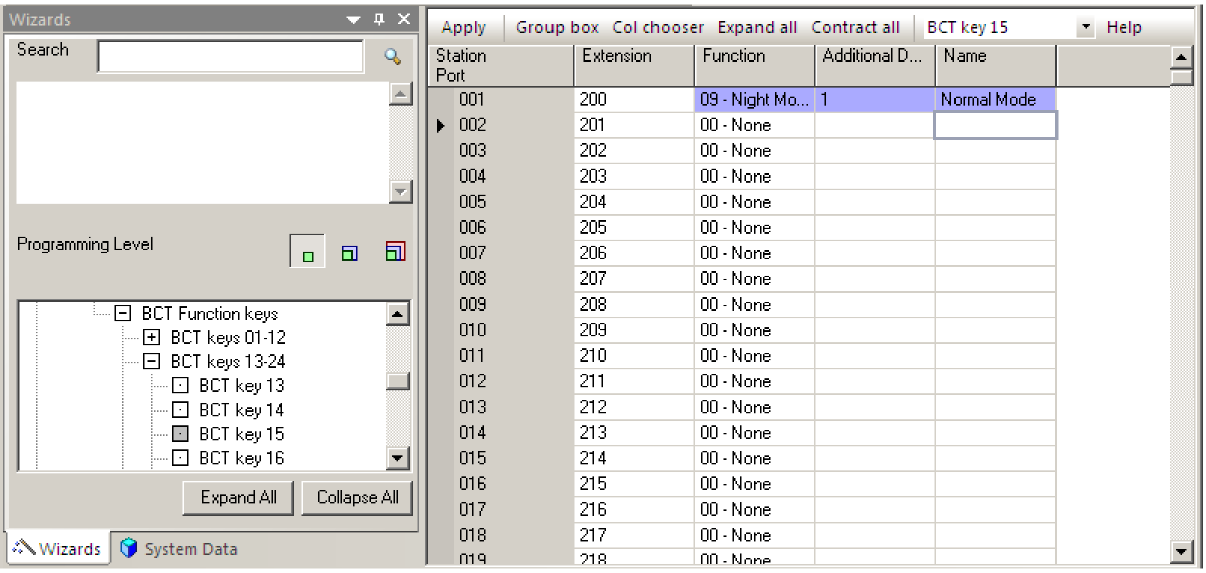
When Resilience mode is active calls to the external Queue and external DDI fail calls are routed to Department group 12, which contains the extension of the operators.

For System Fallback for Contact Center the digits received for Contact Center access should have the System Fallback for Contact Center as Target 1 (e.g. 297). When Resilience mode is active then external calls to the Contact Center will be routed to Department group 11, which contains the extension of the agents.

Note: In this manual, the System Fallback is implemented as a Department group. However, it is also possible to use the Incoming Ring Group feature of the PBX.

Give an extension the right to set Resilience mode and program a FK.

When BCT key 15 is pressed, Normal Mode is activated.

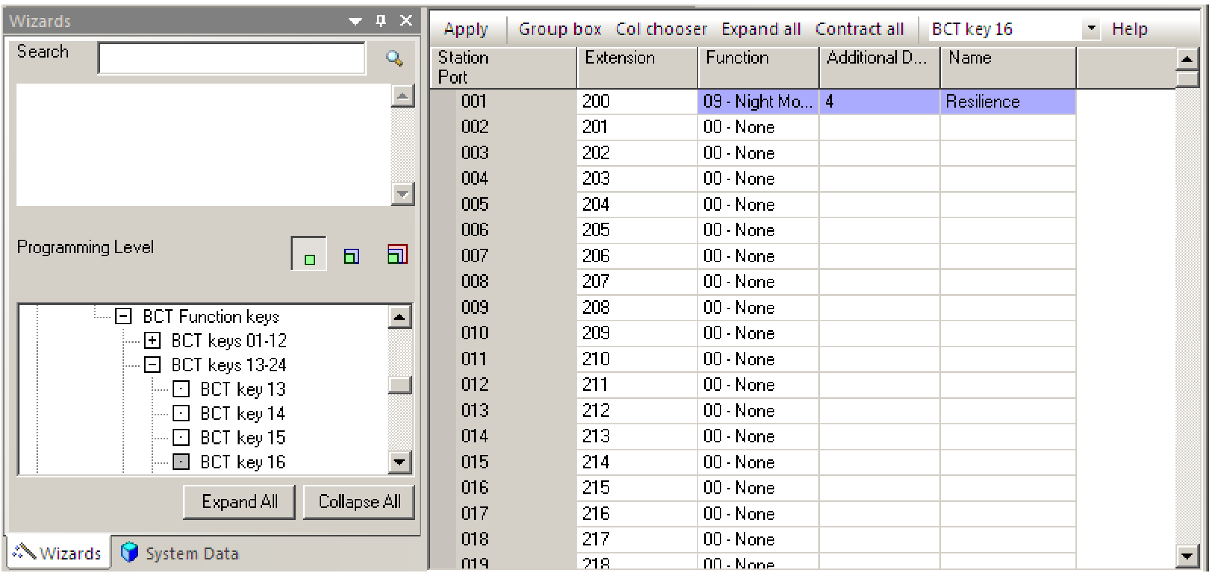


Station Port	Extension	Function	Additional D...	Name
001	200	09 - Night Mo...	1	Normal Mode
002	201	00 - None		
003	202	00 - None		
004	203	00 - None		
005	204	00 - None		
006	205	00 - None		
007	206	00 - None		
008	207	00 - None		
009	208	00 - None		
010	209	00 - None		
011	210	00 - None		
012	211	00 - None		
013	212	00 - None		
014	213	00 - None		
015	214	00 - None		
016	215	00 - None		
017	216	00 - None		
018	217	00 - None		
019	218	00 - None		

Figure 4-32 BCT Key 15

Program Command	Item	Setting
20-06-01 ICM Extension 200	Night Mode	2
20-07-01 Class of Service 2	Night Mode Switching Manual	On
15-07-01 Extension 200 FK 15	Function	09 – Night Mode Switching
15-07-01 Extension 200 FK 15	Additional Data	1
15-07-01 Extension 200 FK 16	Function	09 – Night Mode Switching
15-07-01 Extension 200 FK 16	Additional Data	4

When BCT key 16 is pressed, Resilience Mode is activated.



Station Port	Extension	Function	Additional D...	Name
001	200	09 - Night Mo...	4	Resilience
002	201	00 - None		
003	202	00 - None		
004	203	00 - None		
005	204	00 - None		
006	205	00 - None		
007	206	00 - None		
008	207	00 - None		
009	208	00 - None		
010	209	00 - None		
011	210	00 - None		
012	211	00 - None		
013	212	00 - None		
014	213	00 - None		
015	214	00 - None		
016	215	00 - None		
017	216	00 - None		
018	217	00 - None		
019	218	00 - None		

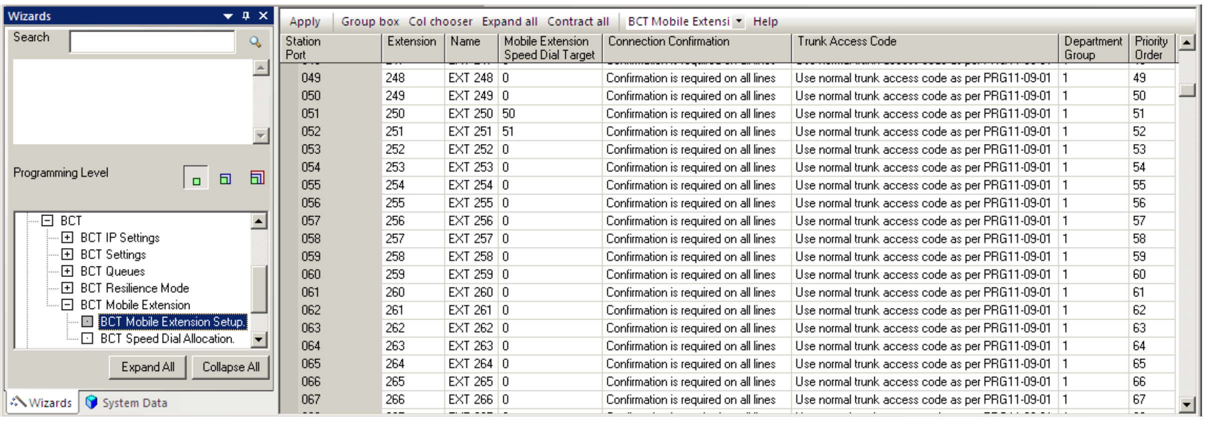
Figure 4-33 BCT Key 16

4.4.4. Mobile extension setup for BCT Mobile Client

The PBX part of the BCT Mobile Client solution (see chapter 8.1.13 BCT Mobile Client application for the Mobile Phone Configuration) is the Mobile Extension. With the Mobile Extension defined, a Mobile Phone can act as a local extension of the SV8100/SV9100.

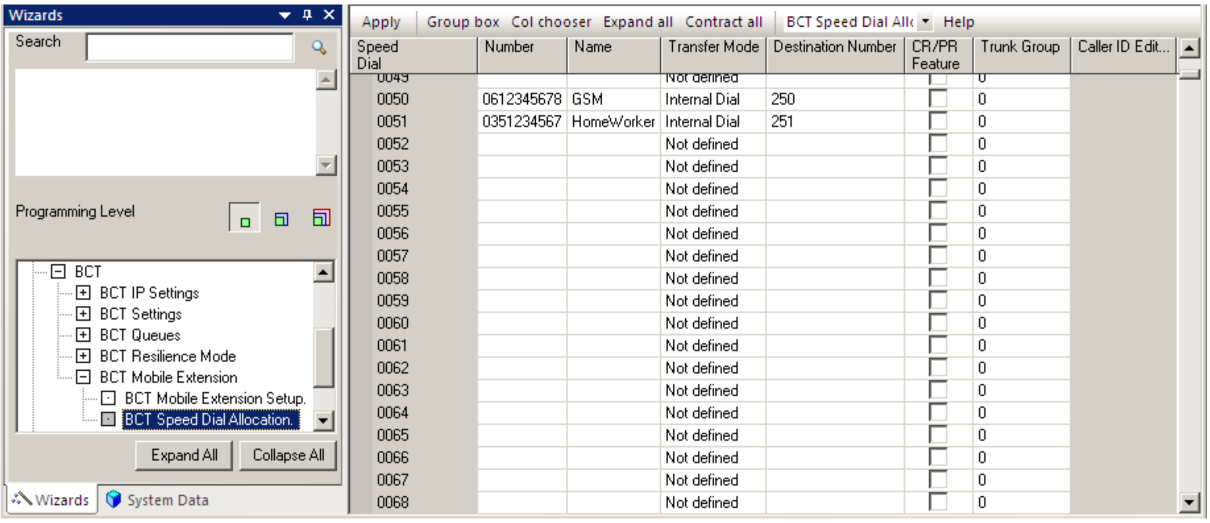
Using PC Pro, open the wizard tab and navigate to **Applications, BCT.**

Define Mobile Extensions as done for 250 and 251 in the pictures below (see special note on "Connection Confirmation" below):



Station Port	Extension	Name	Mobile Extension Speed Dial Target	Connection Confirmation	Trunk Access Code	Department Group	Priority Order
049	248	EXT 248	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	49
050	249	EXT 249	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	50
051	250	EXT 250	50	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	51
052	251	EXT 251	51	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	52
053	252	EXT 252	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	53
054	253	EXT 253	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	54
055	254	EXT 254	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	55
056	255	EXT 255	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	56
057	256	EXT 256	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	57
058	257	EXT 257	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	58
059	258	EXT 258	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	59
060	259	EXT 259	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	60
061	260	EXT 260	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	61
062	261	EXT 261	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	62
063	262	EXT 262	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	63
064	263	EXT 263	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	64
065	264	EXT 264	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	65
066	265	EXT 265	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	66
067	266	EXT 266	0	Confirmation is required on all lines	Use normal trunk access code as per PRG11-09-01	1	67

Figure 4-34 BCT Mobile Extension Setup



Speed Dial	Number	Name	Transfer Mode	Destination Number	CR/PR Feature	Trunk Group	Caller ID Edit...
0049			Not defined		□	0	
0050	0612345678	GSM	Internal Dial	250	□	0	
0051	0351234567	HomeWorker	Internal Dial	251	□	0	
0052			Not defined		□	0	
0053			Not defined		□	0	
0054			Not defined		□	0	
0055			Not defined		□	0	
0056			Not defined		□	0	
0057			Not defined		□	0	
0058			Not defined		□	0	
0059			Not defined		□	0	
0060			Not defined		□	0	
0061			Not defined		□	0	
0062			Not defined		□	0	
0063			Not defined		□	0	
0064			Not defined		□	0	
0065			Not defined		□	0	
0066			Not defined		□	0	
0067			Not defined		□	0	
0068			Not defined		□	0	

Figure 4-35 BCT Speed Dial Allocation

When no Easy Edit is available: Make the Mobile Extension lines 250-251 visible via Programming Unregistered Phones and Mobile Extension List...

Program Command	**Item**	**Setting**
15-22-01 Extension 250	Speed Dial Target	50
15-22-02 Extension 250	Connection Confirmation	Confirmation is required on all lines
13-04-01 Speed Dial 50	Number	0612345678
13-04-02 Speed Dial 50	Name	GSM
13-04-03 Speed Dial 50	Transfer Mode	Internal Dial
13-04-04 Speed Dial 50	Destination Number	250
15-22-01 Extension 251	Speed Dial Target	51
15-22-02 Extension 251	Connection Confirmation	Confirmation is required on all lines
13-04-01 Speed Dial 51	Number	0351234567
13-04-02 Speed Dial 51	Name	Home Worker
13-04-03 Speed Dial 51	Transfer Mode	Internal Dial
13-04-04 Speed Dial 51	Destination Number	251

Note: *With the Connection Confirmation setting you can specify if a user has to press an additional confirmation '*' to accept an incoming call. An additional confirmation prevents that the called party is connected to the voicemail when call setup via the BCT Mobile Client fails or is ignored by the calling user.*

Example: *If Alice calls Bethany via the BCT Mobile Client, then BCT/SV8100/SV9100 will first call Alice and when Alice accepts the incoming call BCT/SV8100/SV9100 will call Bethany and connect both parties.*

However, when Alice doesn't answer the incoming call, the call will be answered by Alice's Mobile Operator voicemail. BCT will now call Bethany and she will hear the voicemail box of Alice which is of course very strange to Bethany.

To prevent that Bethany ends up in Alice's voicemail box in these kinds of call scenarios you can configure the Connection Confirmation to "Confirmation is required on all lines". When set for Alice's Mobile Extension, Alice has to confirm an incoming call by pressing "", only then BCT/SV8100/SV9100 will call the other party.*

In the particular scenario above the voicemail system will never generate "" so Bethany is not connected to Alice's voicemail box.*

When the Connection Confirmation setting is set to "Is not required on all lines" the user doesn't have to press "*" to accept an incoming call, however note that problems can arise as described above.

4.4.5. Headset usage and After Call Work period

Phones with headset (using the headset jack) and using Headset key (05) and Headset Mode (Service Code defined in program 11-11-65), do not return to idle automatically.

Do not use the general Disconnect Supervision ON (program 20-02-09), because this will initiate a new call (give dial tone) after disconnect for non-headset user. For Agents (without headset) this will indicate ending the After Call Work period.

To program return to idle when the call is disconnected automatically for phones with headset do the following:

1. Put phones with headset in a specific class of service (program 20-06)

2. Enable Supplementary Service Disconnect Supervision Enhancement (program 20-13-43) for the used class of service.

Note: When incoming calls are answered via the headphone key on the terminal it is advised to disable 20-13-43 in the specific service class. The consequence is that a disconnected call always should be followed by (manual) pressing the headphone key on the terminal to go to idle condition.
Reason: When 20-13-43 is enabled and an incoming call is answered via the headphone key on the terminal and afterwards the call is disconnected by the calling party, ACW will end due to a very short (but unhearable) dial-tone spike on the terminal (PBX limitation).
When the call was answered via the Speaker-key or with the BCT desktop client the spike will not occur on disconnection and ACW will be started as normal.

4.4.6. Multi-line

Multi-line answer (Hold VE) is only supported for SV8100/SV9100. For SV9100-TAPI Multi-line answer is not supported. Multi-line pickup (Release VE) is supported for both PBX types.

1. For SV8100/SV9100: Program 20-04-01 (VE Option when Answering VE Incoming) :
   Hold VE after incoming call answered or Release VE after incoming call answered.

2. For SV9100-TAPI: Program 20-04-01 (VE Option when Answering VE Incoming) :
   Release VE after incoming call answered

3. Define Virtual extensions, to be used as Lines, in the PBX with command 11-04.

4. Define the Lines on the terminals with command 15-07 (making a relation between VE and button and use *03 - Virtual Extension Key as function).

BCT System Settings (only SV8100/SV9100)

1. Check Enable Multi Line in Connection Tab for the PBX (edit PBX page).

2. Check Enable Multi Line when editing Advanced User Settings in Company Directory for the users using Multi Line.

3. Synchronize BCT.

BCT Client (only SV8100/SV9100)

Now when starting a BCT client, an additional **Lines** view shows the list of lines programmed in the PBX. Lines are displayed in the same order as the buttons which are used on the terminal.

For SV9100-TAPI CAP-keys programmed with 15-07 (value *08) will also be shown in the additional **Lines** view (when multi line is enabled).

To customize User settings for Lines, enter the configuration page and select the Lines tab.

4.4.7. Presence setting to external destinations (AspireX/AspireUX only)

The default way of the AspireX/AspireUX to set call forward to an external destination is using the speed dial functionality. The speed dial is not compliant with active BCT dialing rules.

To use presence setting to external destinations the AspireX/AspireUX must be programmed to set call forwards to external destinations directly:

```
PRG20-01-11 = 1 (Type B) *
PRG20-01-15 = 1 (Type B) *
PRG20-11-12 Call Forward Off-premise = 1 (ON)
PRG20-11-14 Trunk to Trunk Transfer Restriction = 0 (OFF)
*:After the setting change, system reset is necessary.
```

When system option in PRG20-01-11 and 15 is Type A, use program 24-06 to program Call forwards. When system option in PRG20-01-11 and 15 is Type B, use program 24-09 to program Call forwards.

4.4.8. IP DECT

IP-Dect Terminals are registered as SIP or DT700 terminal.

To make BCT automatically detect the correct IP-Dect Terminal type do the following for every IP-Dect terminal:

- Program function key 16 with "*03 – Virtual Extension Key" and own DNR as data.

4.4.9. SV9100-TAPI

- Trunk line keys shall not be programmed on DT700/800/900 telephone sets.

- CAP-keys may be programmed on DT700/800/900 telephone sets. Note that CAP-keys and Line-Keys are only supported when the Operation Mode of the TAPI (3rd party CTI driver) is in Multi Line Mode (default).

- The number plan used for incoming trunk calls should preferably be uniform in length (e.g. for a called party number received on ISDN <area-code><ddi-prefix>xxxx, number length is 4 for all received numbers; the example <area-code><ddi-prefix>yy may not be recognized correctly)

- To prevent barge-in on a conference command 20-13-32 shall be set true

- When using dual-ring, it is preferrable to disable ‘your call has been forwarded’ announcements, command 40-10-10 (or general 40-10-01) should be set to ‘do not play’

- When dual-ring is used to provide forking (two terminals belonging to the same user) it is advised to relate the two terminals also in BCT; see Twinning number in 8.5.1 Extension Configuration (Company Directory).

- Program 20-11-11 (Automatic On-hook Transfer) : Unchecked (mandatory)

- When STD-SIP terminals are used by BCT clients, program 15-05-50 (peer-to-peer) : Unchecked (mandatory)

- Second call for DID/DISA/DIL/E&M (command 20-09-01) is supported (not default). A second external call to a busy extension will be shown as waiting call in the BCT Client. The current call is only visible in the Multi-line tab when the waiting call is answered.

- When BCT needs to work in co-operation with other TAPI applications, the TAPI version to be used might have to be preset to a higher value than the default.
  BCT by default uses TAPI version 2.0 but if other TAPI applications only support version 3.0, BCT needs to start with TAPI version 3.0 as well.
  To have BCT operate with TAPI version 3.0, add the following to the registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Philips\Stsapi Module\Tapi\ InitialTapiVersion] (32 bit OS) or [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Philips\Stsapi Module\Tapi\ InitialTapiVersion] (64 bit OS)
  Add the value as a DWORD and give it value 30.

4.5. iS3000 / SIP@Net configuration

This chapter explains how to set up the PBX type iS3000 / SIP@Net for BCT.
In general where iS3000 is mentioned, also SIP@Net is applicable. However, different terminal types will be used.

Please refer to the Release Notes to check the PBX compatibility.

4.5.1. Script and examples

You can use the script on BCT product DVD (PBX Scripts folder) as a basis for projecting a standalone iS3000 system. The script contains a standard operator, voicemail, and starter entries. Note that the projecting of the iS3000 DOES NOT FOLLOW the examples of the figures in the following sections.

You must change the station numbers (DNRs), hardware addresses etc. to the ones you require.

4.5.2. Configuration overview

4.5.2.1. Operator configuration

The following example shows Operator Routing Points for BCT:

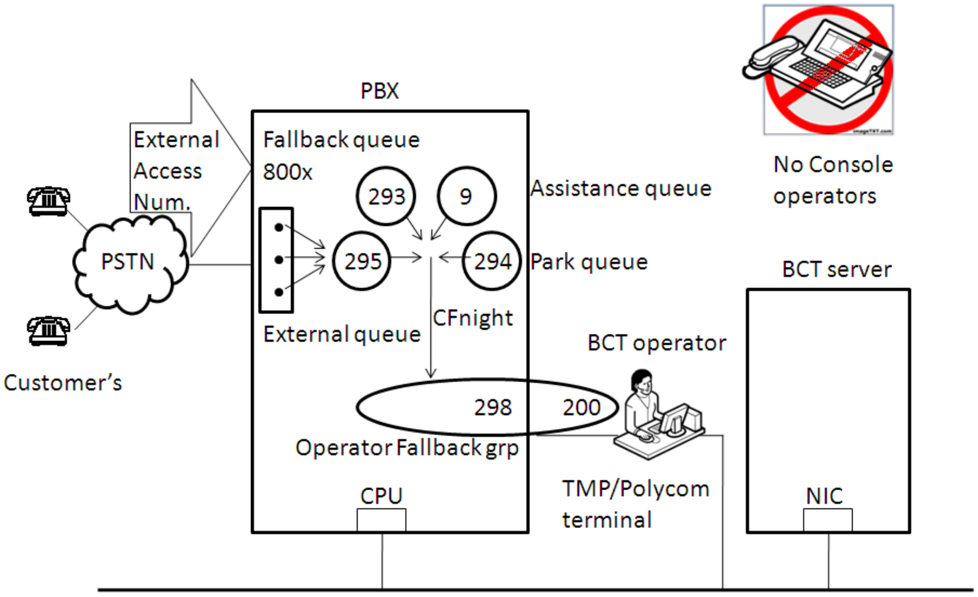


Figure 4-36 Operator Routing Points for iS3000 and BCT

External Access Numbers -> External Queue

Three empty ACD-groups (type=38) are defined as External Access Numbers. These DNRs have call forwarding on night activated to the External Queue. You can distinguish between a general company DNR and, for example, a customer's helpdesk. The operator can see who is being called/what service is required.

BCT-server-down situation

Routing-Point groups are in night-service by default, and are switched into day-service when CTI monitoring is activated for that group and its (agent) state has been changed to Ready (by BCT Server). If the BCT server loses its connection to PBX (server or network down), all groups immediately switch to night service. All BCT-Queues have “call forwarding on night” activated to the “BCT-server-down situation”-group. In this group, all extension DNRs that should handle these calls, are members. Typically these members are the same as the BCT Operators.

Fallback Queue

The fallback Queue is made using the Main Common Night Extension (MCNE). The MCNE is called automatically by iS3000 when there are no iS3000 operators in the system. All external calls that fail (for example busy, non-existent number or not answered) are passed to MCNE. In this scenario the Fallback Routing Point group is assigned as MCNE.

Assistance (Internal) Queue

The ‘9’ in the default projecting number-plan, usually ending at the Operator M-Queue, has been re-projected being a normal internal DNR. This DNR is assigned to the A.Q. Routing Point.

Park Queue

No special requirement except it is a Routing Point group.

4.5.3. Boundaries, options and licenses

BCT requires specific values for boundaries and options, given in this section.

Use the **DIMDAT** command to read the values. If necessary, correct them; do a retrieve, make changes, restore the projecting files into the system and re-project the system. The Second Line Maintenance Manual describes how to do this.

Boundaries

BOUND 231 Max. number of ACD groups (should be equal to or larger than the number of Routing Points, for example 4)

BOUND 276 Max. number of CSTA link per unit. BCT needs one link for the CTI server (and one for CSTA Test Tool if desired). Check the corresponding CSTA license.

BOUND 277 Max. number of CSTA monitored local BSP. This value must reflect the number of DNRs that should be monitored in BCT. Note that *all* DNRs are retrieved from the PBX, not only the voice-DNRs.

Formula for 277 = (all extensions in PBX + RP’s) x1.5

BOUND 279 Max. number of CSTA calls per unit.

Subtract 200 from the value that is defined for Boundary 202 and divide the result by 4.

BOUND 202 Max. number of control blocks. Each monitored extension requires 3 control blocks. Set this to at least 3 times the value of BOUND 277. In addition, add the buffer_pool_occupancy_threshold (boundary 223) plus 200 for internal use:
Formula for 202 = (3 x bnd.277) + 200 + bnd.223
Make sure this fits total memory usage. If this fails, use the maximum possible and adapt boundary 279.

BOUND 328 Max. number of CSTA IO registrations. Same as boundary 277.

BOUND 330 Max. number of CSTA call IDs per unit (always 4096).

BOUND 324 Max. number of sockets per unit.

BOUND 325 Max. number of sockets per task (CPU3000, CPU4000 only).

Options

LOSYSOP 040 Closed number scheme in network must be “YES”.

LOSYSOP 088 Prevent alert from empty S_0 bus must be **“**NO”.

LOSYSOP 091 Unique Dynamic PVN Line Number must be “YES” when (i)PVN is used.

LOSYSOP 116 ACD diversion chaining allowed must be “YES”.

LOSYSOP 117 Absent switching of last ACD member prohibited must be “NO”.

LOSYSOP 119 Unique line numbering must be “YES”.

LOSYSOP 121 PVE Active must be “YES”.

Now it is possible to start the PVE service using OM command **STSRVC**.

```
STSRVC:<IP-SERVICE>[,<UNIT>];
```

where Parameter IP-SERVICE is 0, meaning PVE service.

LOSYSOP 123 PVE short XML must be “YES”.

LOSYSOP 160 Twinning in combination CSTA allowed. This must be "YES" in case twinning is used.

LOSYSOP 161 Multiple Ring group in combination with CSTA allowed must be true when multiple ring groups are used.

LOSYSOP 175 Send cause for CSTA incoming calls must be "YES".

LOSYSOP 177 Check traffic class when set diversion by CSTA must be “No” when set/reset of diversion via CSTA should be independend of traffic classes.

LOSYSOP 196 CSTA Automatic Alerting Generation must be “YES”.

LOSYSOP 206 CSTA via Multi-Unit disabled must be "Yes". Required for correct functioning of DECT Mobility.

LOSYSOP 222	Extended filename-format for voicerecording, required for SIP@Net call recording.

Licensing

The following PBX licenses are required for BCT to work correctly:

- 003 ACD Agent License (Optional)
- 034 CSTA PBC APPL. license.
  A BCT CTI connection requires one license. The CSTA-TestTool requires another.
- 040 CSTA PBC SEAT license.
  Limits the number of monitors that can be started.

4.5.4. PBX configuration

4.5.4.1. General

1. Make an overview of all existing groups:

```
DIGRPA:;
```

2. Correct traffic classes for extension

With the system in night service, the default projecting prevents internal parties from making external calls. Adapt traffic classes by using: CHTRFC:;

3. Enable Facility “Add on entitled” (0) for all DNRs (Employee, Agent and Operator)

4. Disable Facility "Metering" (10) for all Agent and Operator DNRs

5. Ergoline D325/340 Firmware + toggle option

To answer a call using BCT Client, the Ergoline D325-series requires the latest firmware (date: 8-8-2005, v.4.03).

To upgrade, make the firmware available on the LBU/CBU and execute STDOTE;

Note: *This is time consuming (at least 45 minutes), so you can do this after the complete installation if you prefer.*

The firmware is needed for answering calls via CTI-interface. Also check that option “INCOMING INTERCOM” is enabled (ON) in the toggle list of the Ergoline terminal. This is an auto answer for intercom-calls only.

6. Other extension-related facilities

To use facilities like follow-me (for presence), Call Waiting, and AutoRingback, you must assign the appropriate facility to the extension and download the appropriate prefix to the terminal.

For example to use follow-me, assign the Follow-Me facility by using command

```
ASFACM:7,<DNR>;
```

then assign the extension to a download menu by using command

```
CHMDNR:<menu>,<DNR>;
```

Program the function key in this menu and the prefixes to activate and cancel Follow-me by using the following commands:

```
CHFKDA:<menu>,32,0,<data>,3; and
CHFKDA:<menu>,33,0,<data>,3;
```

Finally, download the menus to the extension by using

```
DOWNLD:<DNR>;
```

Note: *To prevent ARB being initiated for Operators and Agents, assign FCM 49. Use*

```
ASFACM:49,<DNR>;
```

Note: *To prevent COB being initiated for Operators and Agents, remove COB. Use*

```
CHCOBD:<DNR>,0;
```

7. User-defined BSPTs

BCT retrieves all DNRs from the PBX (via PVE-link), but only the BSPTs that have a known voice-profile are stored in the database for monitoring. Therefore no user-defined BSPTs should be created and assigned to DNRs that are used for telephony (voice).

However, the PBX offers the use of boundary 282: ProjectedVoiceBSPT which allows you to define your own valid voice BSPT. This functionality is supported in BCT via a setting in the configuration file 'PBXConfigurationService.WinService.exe.config':

- Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\PBXConfigurationService.WinService.exe.config“.
- Locate the key: IS3000.ProjectedVoiceBSPT
- The value “xx” must have the same value as configured for PBX boundary 282. By setting this value, BCT will also accept DNRs with this custom voice BSPT.
- Press Save to store the value.

Note: *To prevent COB being initiated for Operators and Agents, remove COB. Use:*

```
CHCOBD:<DNR>,0;
```

After changing the configuration file you should synchronize again.

4.5.4.2. Twinning

To use Twinning, you must:

1. Make sure that option 160 is set. See 4.5.3 Boundaries, options and licenses.
2. Define a (bothway) Twinning relation between 2 extensions.
   Example for extensions ExtA and ExtB:

```
CRTWIN:<ExtA DNR>,<ExtB DNR>; // From ExtA to ExtB:
CRTWIN:<ExtB DNR>,<ExtA DNR>; // From ExtB to ExtA:
```

   Note that you must also define this in BCT; see Twinning number in 8.5.1 Extension Configuration (Company Directory) .

4.5.5. PBX configuration for the Operator

4.5.5.1. Put iS3000 in night service

Make sure there are **no** active operators in an iS3000 system to which a BCT Operator is connected:

- De-activate all iS3000 operators
- Make special extensions INE, PLE, and SCNE absent

This puts the system in night service, so all operator calls go to the Main Common Night Extension (MCNE). In addition, non-DDI calls seeking assistance go to MCNE.

Note: *Pay attention to **Traffic Classes** for terminals and trunks with the system permanently in night service.*

4.5.5.2. Program Operator Routing Point

1. Make an overview of all existing groups

```
DIGRPA:;
```

2. Remove '9' from number plan

By default, when '9' is dialed, the call is put in the operator M-Queue. Remove this by using:

```
MAKENU:0,9;
```

3. Ensure all BCT operators use a set that has auto-answer and can handle a headset (for instance a TMP-terminal Ergoline D+325/340 or a Polycom set)

These terminals are capable of advanced call manipulation via CSTA interface.

4. Create all Queues (groups) by using:

```
CRGRPA:<QUEUE-DNR>,<TYPE>;
```

Use type 59 for the special Routing Point Group, and use another type for the Fallback group used for the BCT-server-down situation, for example 15 (depending the needs for distributing calls – hunting, fixed, cycle or multiring).

If you only want one DDI-point and no flexibility for multiple DDI's, then the 'external queue'-DNR can be the DDI. In this case, Figure 4-36 Operator Routing Points for iS3000 and BCT changes in such way that the multiple DDI-points can be removed.

For type 15 group, add all DNRs you want to assign to the Fallback group used for the BCT server-down situation. Typically these are the DNRs belonging to the BCT Operators

For type 59 groups, use all defaults except for:

```
Enter Full Threshold [<ACD-THRESHOLD>]: 99nn; See note for 'nn'
Enter Busy Threshold [<ACD-THRESHOLD>]: same as above
Enter Pause tone [<ANN-PAUSE-TONE>]: MOH for PARK-Q, others
 using internal ring tone
```

Note: *The "nn" must have minimum value of 20. The 'nn' represents the (COB) depth of the Queue, the amount of external calls it can hold. This value can be the same for all Queues, but typically the "External Calls"-Queue is bigger. The depth of the external Queue must be at least the amount of trunk lines available for incoming calls.*

From SIP@Net version 862.00.0 and later parameter 'nn' can have values 01 upto 200 (nnn), the maximum is specified by system boundary 466 MaxNumberOfCallsOnRoutingGroup with default 97. Setting this maximum value higher than the default is only allowed for SIP@Net server.

5. Assign fallback

   For all groups except the Fallback, assign "Call-Forwarding on Night" to the operator fallback group.

```
CHCALF:5, <QUEUE-DNR>,<OP_FALLBACK-QUEUE>;
```

If the BCT Server loses its connection to the PBX, the group is automatically put in night service and all calls are routed to the Fallback group.

6. Assign facility for correctly filled in CTI events
   Assign facility 47 (overrule CLIR) for all Routing Point groups:

```
ASFACM:47,<DNR>;
```

4.5.5.3. Call routing

Operator Assistance

Since the '9' has been removed from the number-plan and a new group is created using this number, it is now added to the number-plan analysis as internal number.

```
ASBLCK:0,9,1,1,10;
```

Fallback for external calls

Assign the Fallback Queue as MCNE:

```
CHMCNE:2,<FALLBACK_Q_DNR>; (293).
```

Since you want all assistance handled via the BCT Operator, INE, PLE and SCNE should also be absent.

In case of an iS3000 network, when all BCT operators are absent or if a specific BCT server/CTI-link is out of service, the assistance of calls can be rerouted to an alternative PBX within the iS3000 network. This is done by using "Call Forwarding When Night" of the Routing Point. In both cases the iS3000 handles the rerouted calls as the SIP@Net operator Queue diversion functionality.

Check the General and DDI-options for the trunks that operator assistance is used for the different failures. Use the OM-commands: DIROUT, CHRTCI and CHRTCG.

DDI points for external queue

This only applies if you require flexible multiple DDI points.

Create via CHDNRC: hardware less extension to be used for General Access Number(s). In the example in Figure 4-36 Operator Routing Points for iS3000 and BCT, these are: 8000, 8001 and 8002. For all these DNRs, assign call forwarding on Not Reachable to the External Queue:

```
CHCALF:8,<DNR>,<QUEUE-DNR>;          (e.g. CHCALF:8,8000,295;)
```

Call Completion / COB queues

The BCT Operator can transfer an external call to a busy internal party. To make this work, you must assign and enable a COB-Queue (If transfer fails because of no COB or full COB, the CTI-action returns an error, and the BCT Operator receives an error popup).

It is not mandatory to assign the start COB entitled facility to all BCT Operator DNRs:

```
ASFACM:36,<operator DNR>;
```

When an operator is logged-in in the BCT client, COB can be started without FACM 36 when a busy destination is met.

It is possible to (re)assign a short- or long COB-Queue to any DNR. In the default projecting a short COB-Queue can hold 5 calls and long can hold 10 calls. (Boundary numbers 216 and 217).

To check and modify COB-Queues, use:

```
DICOBD:<DNR>; and
CHCOBD:<DNR>,2;
```

Note: *Make sure that the Route/Bundle/Line combinations are unique. The Route/Line information is used in case of fallback situations.*

Correct the route options for DDI-route

In addition to regular settings for correct operator assistance, BCT Operator requires the following DDI and tone options for incoming (DDI) calls:

- GEN-TONE (via CHRTCG)
  The 'tone type for COB after answer' must be '1 = MOH or waiting tone'
- TONE-AND-DDI-OPTS (via CHRTCI)
  Route all DDI-fail actions (option T up to X) to the Operator / Assistance (9)

ReCall

Recall is a situation where a transferred or parked party is automatically transferred back to the terminal that handled this call before. This is performed by the PBX and can be configured.

This situation is actually unwanted, since the BCT Operator performs this action via his/her own terminal. A regular ReCall goes directly to this terminal, bypassing the BCT Operator's Queues.

Different scenarios:

- ReCall from a party put on HOLD and not retrieved after time-out
- ReCall from a party that has been put into the PARK-Queue and not picked up after time-out.
- ReCall from a party that is transferred but other party didn't answer within time-out.

By default on iS3000 this functionality is disabled, and should remain disabled.

Break in

The BCT operator can break-in into a busy party. To make this work you must assign Break-in to the DNR'S of all BCT operators.

It is not mandatory to assign the Break in entitled facility to all BCT Operator DNRs:

```
ASFACM:2,<operator DNR>;
```

When an operator is logged-in in the BCT client, Break in can be started without FACM 2 when a busy destination is met.

To allow operators to break in and claim a busy trunk line, each operator DNR needs to be assigned facility class mark 61.

```
ASFACM:61,<operator DNR>;
```

Call Recording

The BCT operator can record a call. See chapter 4.5.12, Call Recording on how to configure this.

System Call Park (also called Pickup Park)

To use the System Call Park functionality for operators a separate set of Routing points need to be configured. Every System Call Park position requires a separate Routing point.

Ceate an ACD group using type 59:

```
CRGRPA:<QUEUE-DNR>,59;
```

When prompted, use all defaults except for:

```
Enter Full Threshold [<ACD-THRESHOLD>]: 99nn;
Enter Busy Threshold [<ACD-THRESHOLD>]: same as above
Enter Pause tone [<ANN-PAUSE-TONE>]: MOH for PARK-Q, others using internal ring
tone
```

For specification of ‘nn’ see paragraph 4.5.5.2 Program Operator Routing Point

Finally assign overrule CLIR facility for the created ACD groups.

```
ASFACM:47,<ACD group DNR>;
```

The ACD groups will now be seen as routing points by BCT and can be used for System Call Park. For BCT configuration for System Call Park see 8.3.10 Create System Call Park configuration.

4.5.5.4. BCT Operator in PBX networks

BCT can be used as central operator in an iS3000 network. BCT supports both closed numbering plan and open numbering plan. It should be possible to call all desired numbers from any iS3000 in the network, e.g. operator Queues, extensions of clients and trunk access codes. This means that numbers that do not reside in a local PBX should be routed over VPN to the PBX where the number resides. For open numbering plan the number should be preceded by the cluster id of the iS3000 where the number resides. Although BCT physically accesses only one iS3000 for the operator routing points and the VMP lines, the iS3000 network logically behaves as a single PBX.

Every iS3000 network node requires its own cluster identity. Assign the cluster identity by the OM command:

```
CHCLID: [[<CLUSTER-ID>] [,<ASSISTANCE-POINT>[,<LOCAL-OPERATOR-MARK>]]];
```

CLUSTER-ID is the unique number by which the system can be reached by other exchanges. Note that this cannot be the same as the first digit(s) of the DNRs in your system, e.g. if the DNRs in your system are 1xxx and 2xxx, the CLUSTER-ID cannot be 1 or 2.

ASSISTANCE-POINT defines where operator assistance should be given. This should be the cluster ID of the iS3000 where the routing points of BCT operator are defined.

LOCAL-OPERATOR-MARK should be set to No to route operator calls to other iS3000 Nodes.

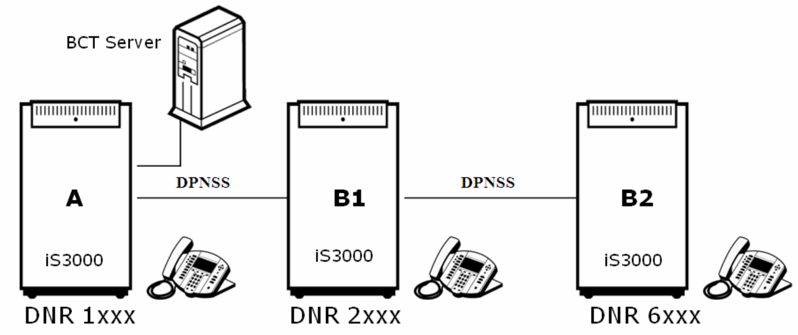


Figure 4-37 Multi-iS3000 environment

In node A, create:

- Routing Points for all Queues (internal, external, fallback, park), as described in section 4.5.5.2 Program Operator Routing Point
- In the OM command CHCLID ID the Assistant point should be the same as the cluster ID itself.
- Set option 174 “Operator queue diversion allowed” to YES.

In the nodes B:

- In the OM command CHCLID ID the Assistant point should the cluster ID of node A.
- set option 174 “Operator queue diversion allowed” to YES.

On the DPNSS route between the iS3000 nodes change the General Route options:

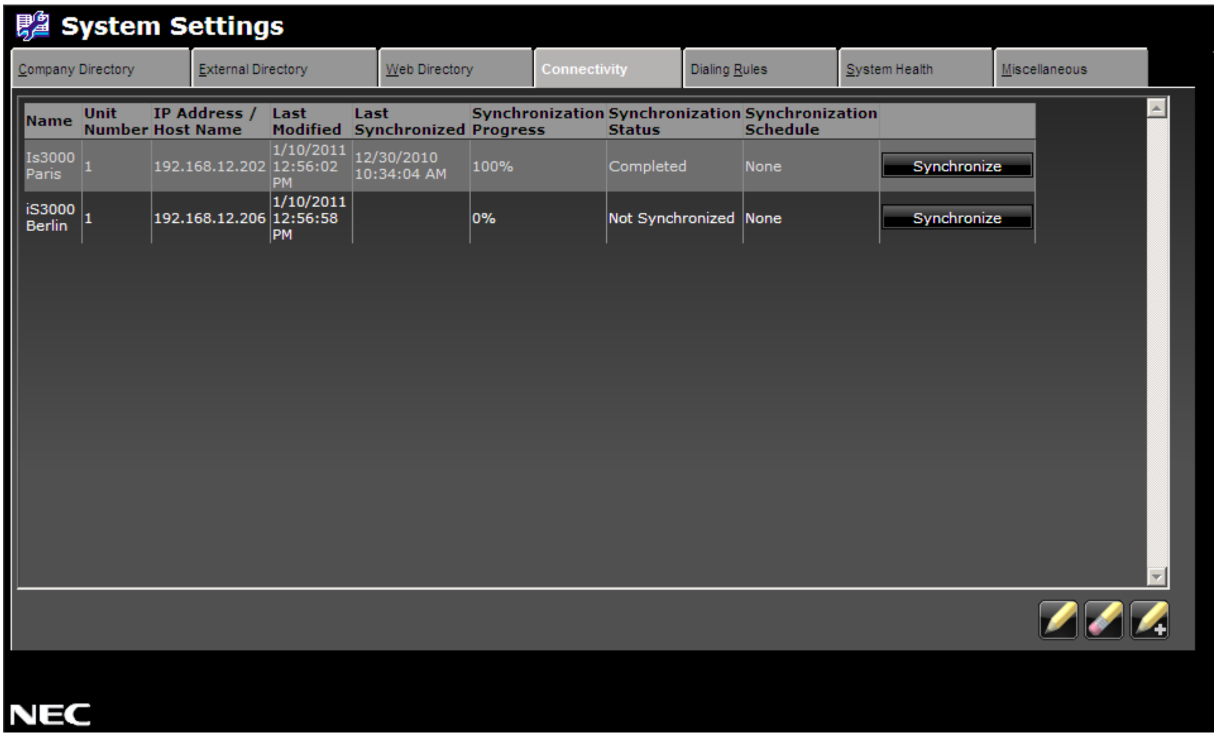
- “Assistance required” (option Q) to 1 = Yes.
- “Flexible operator assistance available” (option W) to 1 = Yes.

See the iS3000 “Operator Facility Implementation manual”, chapter “Assistance in a DPNSS Network” and the iS3000 “Network routing facilities Explained” , chapter “iSNet Wide Area Network” for more information.

***Note:** So-called “mixed mode” (manipulate a call via CTI, that has not been set up by CTI) is not supported.*

***Note:** CTI based Break-In and Camp-On-Busy are not supported for “predictive calls”.*

When BCT is installed, all used PBXs are defined in the Connectivity tab and synchronized. See section 8.1.5 Connection to PBX for information on the Connectivity tab.



Name	Unit Number	IP Address / Host Name	Last Modified	Last Synchronized	Synchronization Progress	Synchronization Status	Synchronization Schedule	
Is3000 Paris	1	192.168.12.202	1/10/2011 12:56:02 PM	12/30/2010 10:34:04 AM	100%	Completed	None	Synchronize
iS3000 Berlin	1	192.168.12.206	1/10/2011 12:56:58 PM		0%	Not Synchronized	None	Synchronize

Figure 4-38 System Settings Multi-iS3000 connectivity

4.5.5.5. BCT operator in mixed network

In a mixed network the iS3000 will be the Home PBX (PBX-A). The Home PBX contains all the operator Queues, IVR-lines, Voicemail number and access numbers. BCT only sees the home-PBX as if it were a stand-alone PBX. The other PBXs in the network (the Remote PBX-B) should route calls to operator Queues and access numbers to the iS3000 Home PBX-A via CCIS.

Note: *If PBX-B has an operator phone connected, another (second) Park Queue must be created on PBX-B. Make sure that in this Park-Queue no prompts are played.*

Note: If CCIS is used on PBX-A (iS3000), then option 183 "CCIS Number Presentation Restriction" must be On.

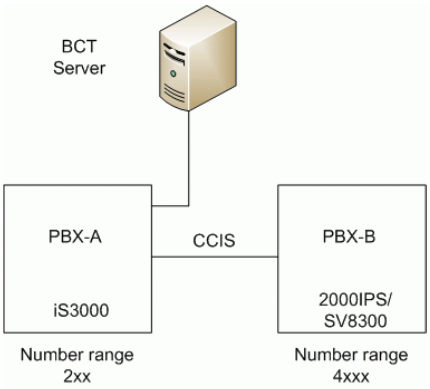


Figure 4-39 Mixed iS3000 environment with SV8300/SV9300

In the iS3000, PBX A, create:

- Routing Points for all Queues (internal, external, fallback, park)
- IVR group(s) and access numbers, as described in section 4.5.5.2 Program Operator Routing Point

In the SV8300/SV9300, PBX-B:

- Create a Virtual extension. This extension will be used to handle unsuccessful calls (DDI-Fail actions).
- Only project the DDI fail actions for DID destination Unassigned numbers and DID destination DND numbers to this Virtual extension:

11 > 520 > 4099	Create Vitual extension to handle DDI fail actions
5100 > 01 > CCC	No Answer, DDI calls: no action.
5101 > 01 > CCC	No Answer, tieline calls: no action.
5102 > 01 > CCC	No Answer, station calls: no action.
5103 > 01 > CCC	Busy, DDI calls: no action.
5104 > 01 > CCC	Busy, tieline calls: no action.
5106 > 01 > 4099	Unassigned Number. DDI calls: forward to 4099
5107 > 01 > CCC	Unassigned Number. tieline calls: no action
5108 > 01 > CCC	Unassigned Number. station calls: no action
5110 > 01 > 4099	DND, forward to 4099

- Set Forwarding-All from this Virtual extension to the operator fallback Queue in the iS3000
  E600>4099>2,93 (293=operator fallback Queue in iS3000)
- For DDI Destination to Busy and No Answer calls Split call forwarding will be used. This should be programmed on all extensions:
  08 > 241 > 1;
  08 > 600 > 0;
  08 > 608 > 1;
  08 > 564 > 0;

6523 > 01 > 1	Split forward 'off' for internal calls;
6524 > 01 > 0	Split forward 'on' for C.O. calls (DDI);
6525 > 01 > 1	Split forward 'off' for tieline calls;
E604>extension>8	Go to normal forwarding for the extension;
E605>extension>8	Go to destination of block 0 for Busy/No Answer of C.O. calls (DDI) for extensions;
78 > 010> 2.93	Set forwarding for block 0 to operator fallback Queue;

Note: *When BCT is installed, all used PBXs are defined in the Connectivity tab and synchronized. See section 8.1.5 Connection to PBX for information on the Connectivity tab.*

The following picture shows SV8500/SV9500 environment:

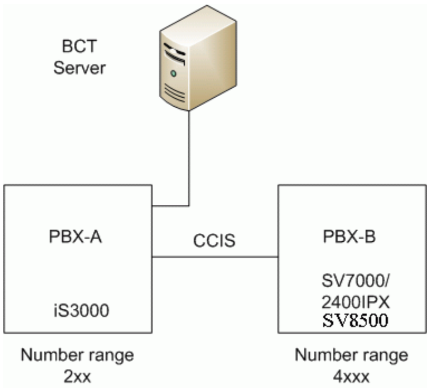


Figure 4-40 Mixed iS3000 environment with SV8500/SV9500

Take care that routing from the SV8500/SV9500 to IS3000 is possible. Program the configuration of the above picture:

In the iS3000, PBX A:

- create Routing Points for all Queues (internal, external, fallback, park) IVR group and access numbers, as described in section 4.5.5.2 Program Operator Routing Point
- create hardware-less DNRs. This DNR will be used to handle unsuccessful calls (DDI-Fail actions).
- only project the DDI fail actions for DID destination Unassigned numbers and DID destination DND numbers to this hardware less DND, for other DDI fail see next part:

In the SV8500/SV9500, PBX-B:

- Define DDI fail actions:

  Program the number to which failed calls should be routed first

  ASDT TN=1, STN=297, LENS=073243, TEC=18, RSC=1, SFC=1
  ALGSN TYPE=2, UGN=1, TELN=297, FPC=1, TN=1, STN=297

  Set CF All for 297 to the Monitored number 2502 (the fallback Queue in the IS3000)

  ACFS_T TN=1, TELN=297, press Get, select radio buttonTYPE = 'Call Forwarding' and SRV = 'All Calls'. Fill in for CFD 2502 then press Set and Exit.

  Program the fail actions to be forwarded to 297

  ACFON TN=1, CF Busy Line, CFI=TELN, UGN=1, TELN=297
  ACFON TN=1, CF Don't Answer, CFI=TELN, UGN=1, TELN=297
  ACFON TN=1, CF Intercept, CFI=TELN, UGN=1, TELN=297
  ACFON TN=1, CF Logout, CFI=TELN, UGN=1, TELN=297
  ACFON TN=1, CF Incomplete Number, CFI=TELN, UGN=1, TELN=297
- Shorten the CFNA timers for 297 to improve rerouting time to operator for external calls to busy extensions:
  ADAI_T MODE select radio button MODE=TELN, enter UGN=1 TELN=297, then press Get, then enter for CDN value 7 (139TC) the value of 1. All other CDNs must be left at value 0. Press Set.

4.5.6. PBX configuration for Contact Center or Voicemail

This section explains how to setup the iS3000 for a BCT Contact Center that makes use of IVR for queuing.

4.5.6.1. General

To understand the PBX configuration, requires understanding how BCT is connected to the PBX. Figure 4-41 Group Configuration shows an example of a configuration. Based on this example, this chapter explains how to setup the system.

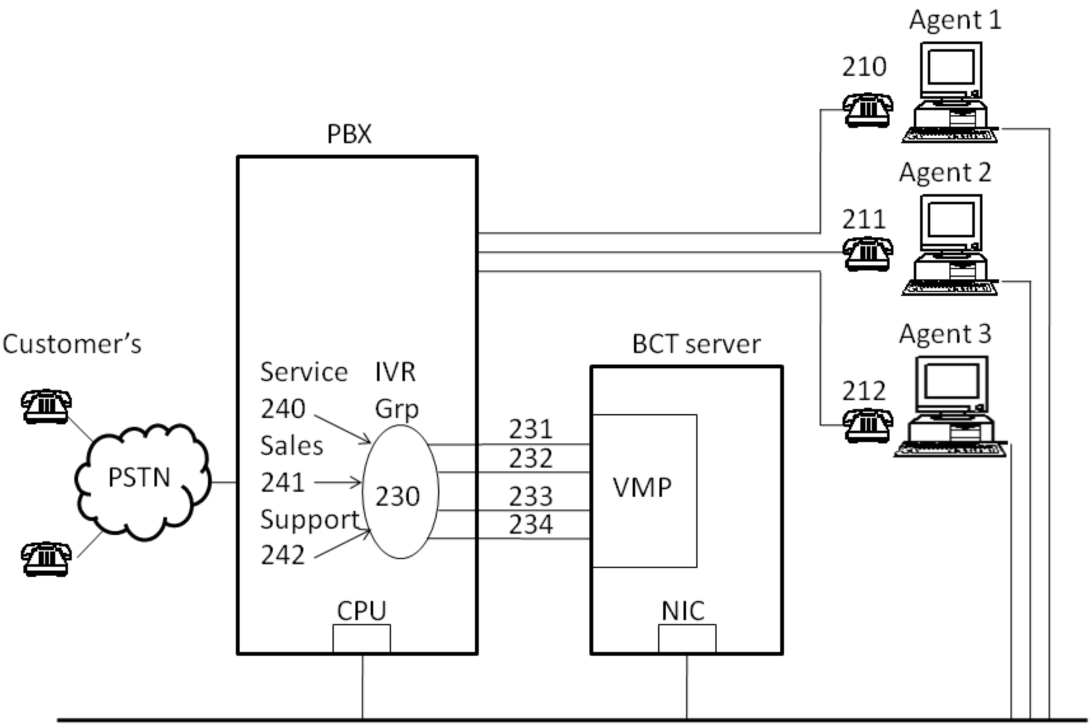


Figure 4-41 Group Configuration

The following items are important:

- BCT takes care of the routing to the agents.
  This means that the ACD functionality in the PBX is not used!

- The login/logout status of the agents is exchanged by means of the CTI connection. Agents can switch ready/not ready or login/logout via dialing a special DNR or via their PC.

- BCT takes care of queuing.
  Calls are queued in BCT and NOT in the PBX. However, for each call that is in the BCT Queue, one VMP line between BCT and the PBX is occupied.

- BCT plays announcements.
  Only the announcements of the BCT are used.

- BCT receives extension status information via the CTI connection.

- As VMP line between BCT and the PBX a Voice Media Port (VMP) is used. In iS3000 the VMP is implemented by a SIP extension.

In summary: the ACD functionality in the PBX is not used at all. BCT uses normal extensions as agent extensions. These extensions are only placed in an ACD group when creating a fall back scenario.

4.5.6.2. Status switching of phone based agents

Agents can change their status (Logon, Logoff, Ready, Not ready and Work ready) by using one of the following methods:

1. Call a Logon Starter Line (can only be used with IVR configuration)

2. Dial an agent status switch access prefix

Each method requires its own programming in the PBX.

4.5.6.2.1. Agent status switching using Starter Line

In case of a Logon Starter Line, the agents need to dial a special number for changing their status. Figure 4-42 Agent login/Logout, Ready/Not Ready switching shows the structure for agent login/logout and switching ready or not ready.

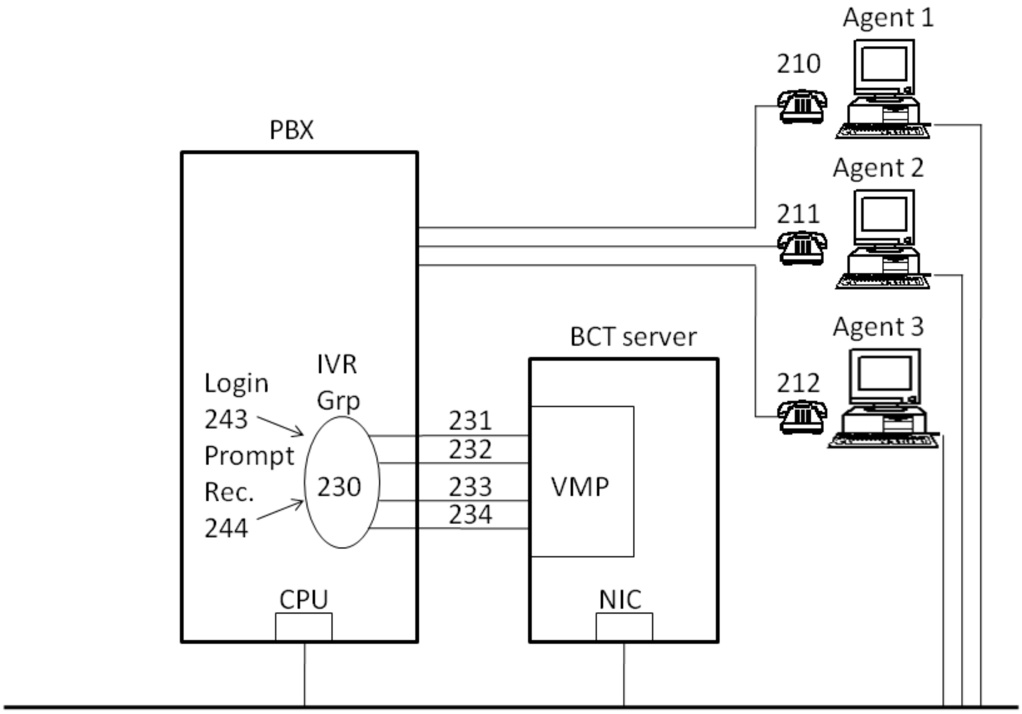


Figure 4-42 Agent login/Logout, Ready/Not Ready switching

When an agent needs to change the status, the agent dials a special DNR. This special DNR is a hardware-less DNR with a Call Forwarding on Not Reachable to the IVR Group. Via the IVR group an VMP line to BCT is selected. It is also possible to create a “Non member group” with Call Forwarding When Night to the IVR group.

For creating the Agent Logon starter line within BCT see 8.2.5 Phone-based agents

If your system is a busy system, it can be useful to use a dedicated VMP line. This means that the line is no longer available for BCT access. You must remove that line from the IVR Group. You must also assign the CFWN relation to the DNR of the dedicated VMP line. Also in this case, the Hardware less DNR should be assigned in the "Starter Module" in the BCT Supervisor Dashboard.

4.5.6.2.2. Agent status switching using access prefixes

Phone based agents use prefixes to logon and log off. Entering call type information and switching not ready is also possible via prefixes.

Note: *Entering status information is only applicable for Phone Based Agents.*
Computer Based Agents use the application to change the agent status.

There is one exception.
In case of Fallback, no Computer Based Agents are available any more. In that case the agents configured for the Fallback group(s) must login and switch themselves ready by entering status information.

The "ACD server dialed" prefixes must be defined with the **CHCSDD** command.

```
CHCSDD:<TREE>,<NUMBER>,<TRFC><<SERVER_AND_ACTION_CODE>,[,[<PW_NMB_LENGTH>]
[,<ADD_INFO_NBR_LENGTH>]];
```

- **TREE**: Destination tree "0" (initial) and/or "1" (inquiry).
- **NUMBER**: The prefix that agents or supervisor dials for a certain action. These numbers should be "easy" to remember, for example "*31" Agent login and "#31" agent logout.
- **TRFC**: The required traffic class, most of the time the traffic class for agents are low.
- **SERVER_AND_ACTION_CODE**: Server and action codes are used by two types of applications. Message Server and ACD MIS Server. First you have to select for which Server the action is valid. Select 1 (ACD MIS server code) followed by the required action code:
    - 1=Agent logout;
    - 2=Agent not ready;
    - 3=Agent ready;
    - 4=Agent login and ready;
    - 5=Entering transaction code
- **PW-NBR-LENGTH**: No password number length must be entered
- **ADD-INFO-NBR-LENGTH**: This parameter defines the number of digits that must be entered for the above mentioned actions. As an example: an agent login is configured with the number "*31" to identify the agent the agent PIN (3-6 digits) must be entered after the "*31" in this example the **ADD-INFO-NBR-LENGTH.**

  Table 4-2 Number of digits per action explains the number of **ADD-INFO-NBR-LENGTH** digits per action.

  The number of digits used for the "not ready reason" and the "call type" should match the number of digits that are used during the creation of these items. For more information see BCT Administrator Guide Chapter "Not Ready Reasons".

ACTION CODE	ACTION CODE DESCRIPTION	NUMBER OF DIGITS
1	Agent logout	-
2	Agent not ready (Not Ready Reason)	0-6 (default 1)
3	Agent ready	-
4	Agent login and ready (PIN code)	0-6 (default 3)
5	Entering transaction code(Call Type)	0-6 (default 1)

Table 4-2 Number of digits per action

Already created prefixes can be displayed with the OM command **DICSDD**.

4.5.6.3. Codes for phone based agents

In case the required agent status is logon, a PIN is requested to identify the agent. How to configure the a phone based agent with PIN in BCT, see 8.5.10 Manually create a BCT user the Agent by Phone parts. Be aware that the PIN length configured within the switch must be the same as the length of the PIN configured within BCT.

In case the required agent status is logged-on, a PIN is requested to identify the agent. For information on how to configure a phone based agent with PIN in BCT see 8.5.10 Manually create a BCT user – the Agent by Phone parts.

In case the required agent status is not ready, a Not Ready Reason (NRR) is requested to identify why the agent is switched not ready. Not Ready Reasons (NRR) are entered in tables in the Business ConneCT Database via BCT Supervisor Dashboard. The information in the **Dial Code** column references the chosen Additional Info digits. After installation, a number of default NRRs are available in the chosen system language. In this example the English NRRs are given with their default dial codes:

Not Ready Reason	Dial Code
Coffee break	1
Lunch	2
Other work	3
Personal affairs	4

For more information on how to configure Not Ready Reasons in BCT, see chapter “Not Ready Reasons” in BCT Administrator Guide.

In case the required agent status is ready, a Call Type (CT) is requested to identify the type or outcome of the handled call. Call Types (CT) are entered in the Business ConneCT database via BCT Supervisor Dashboard. The information in the Dial Code column references the chosen Additional Info digits. After installation, a number of default CTs are available in the chosen system language. In this example the English CTs are given with their default dial codes:

Call Type	Dial Code
Successful	1
Unsuccessful	2

For more information on how to configure Call Types in BCT, see chapter “Call Types” in BCT Administrator Guide.

***Note:** A code is always terminated with a # !*

4.5.6.4. PBX configuration for Voicemail

To use the integrated BCT voicemail system, the following items must be configured on the PBX:

1. Create an IVR group with VMP lines.

2. Project a DNR as Voicemail access number.
   This is a dedicated hardware-less DNR with a Call Forwarding on Not Reachable to the IVR Group.

3. Specify this DNR as Messagebox access DNR in the BCT Supervisor Dashboard.

4.5.6.5. Configuring the BCT Lines in the PBX

***Note:** In the following program example is assumed that a Fallback scenario is used as described in chapter 4.5.6.6 PBX Configuration with Fall Back Scenario. When no Fallback is required the IVR hunting groups is the entry (starter) number for the callers.*

The VMP lines in iS3000 are implemented as SIP extensions. Execute following procedure to configure the SIP lines in the PBX:

1. Assign virtual SIP extension board. Use OM command **ASBRDS**. Example:

```
ASBRDS:15,2,39,B001,255,1;
```

2. Define the signaling group in which the CODEC assignment and Payload are specified. Use OM command **CHIPPD**.

Example:

```
CHIPPD:b001,4,0; (4 means codec specification)
CHIPPD:b001,5,30; (5 means payload)
```

We recommend using G711/30ms, system wide. See 4.1.1 Using VMP lines for IVR. However, if the customer already uses G729, and wants to keep it, you can use G.711/30ms as the second choice. To create a signaling group with first priority G729 and second priority G711/30ms, use the following command:

```
CHIPPD:b001,4,3,0;
```

3. To be able to select menus (post dialing) it is necessary to assign RFC2833:

```
CHIPPD:b001,6,1;
```

4. To activate the changes, the command **SETINS** must be given. Example:

```
SETINS:15,2;
SETINS:15,2,0&&31;
```

5. Assign the DNRs of the SIP extensions to the virtual circuits, for example:

```
CHDNRC:231,15,2,0;
```

Note: *When using SIP, the "user" (application or human) can be asked to logon the SIP extension during the registration process. When an application like BCT is used, make sure that no SIP user credentials have to be entered. Currently BCT is NOT able to logon SIP extensions. With the command DISUSR you can check if logon is required.*

Note: *For connecting SIP phones and lines, an ISG board is required. For more information please refer to the "SIP Trunks and Extensions - Customer Engineer Manual".*

After creating the SIP extensions execute the following procedure to configure the extensions as VMP lines for BCT:

1. Assign Facility Class Mark 32 (post dialing) to **each** SIP extension used for VMP line. Example:

   ```
   ASFACM:32,231&&234;
   ```

   Note: *NEVER assign FCM 33 (VoiceMail Server) to the Lines! If you assign this FCM to the lines, the system will not work.*

2. Assign FCM 47 (overrule CLIR) to each SIP extension used for VMP line. Example:

   ```
   ASFACM:47,231&&234;
   ```

3. If you want to suppress agent number display on the VMP lines, assign FCM 51 (COL permanently restricted). Use OM command **ASFACM**. Example:

   ```
   ASFACM:51,231&&234;
   ```

4. Put the VMP lines that are used for customer calls into a hunting group in the PBX. Use OM Command **CRGRPA** with group property **17**. Example:

   ```
   CRGRPA:230,17;
   231,0,0;
   232,0,1;
   233,0,2;
   234,0,3;
   ```

5. If you need more than one access number (more than one service requested), create dummy DNRs (no hardware associated) with "call forwarding not reachable" to agent ACD group. Example:

   ```
   CHDNRC:24x,12,,2; You can use a circuit number that does not have hardware.
   CHCALF:8,24x,230;
   ```

   Non member ACD groups can also be used for this purpose. Create one or more non member ACD groups and set call forwarding to the agent ACD group.

4.5.6.6. PBX Configuration with Fall Back Scenario

For safety reasons it is recommended to configure a Fall Back option. BCT takes over the call distribution from the PBX. If for whatever reason BCT server is down or cannot be reached, all calls will be lost. Therefore it is strongly recommended to configure a Fall Back scenario. There are two types of Fall Back configurations possible.

Manual Fall Back

The VMP lines are collected in a Basic hunting group. The agents are grouped in an ACD group. A call forwarding when night is configured from the agent ACD group to the IVR hunting group.

In normal operation the agent group is switched to night. All calls are forwarded to the IVR hunting group. When the BCT server is down or cannot be reached, the Supervisor of the Contact Center must switch the agent ACD group from night to the day status. From this moment on the calls will be distributed to the agents of the ACD Group.

The moment BCT is operational again, the supervisor must switch the ACD group back to night. From that moment on, BCT is in normal operation.

Configuring manual fall back is described in section 4.5.6.7 Configure Manual Fall Back.

Automatic Fall Back

Just like the manual Fall Back, the IVR lines are grouped in a hunting group and the agents are grouped in an ACD group. The difference is that in an automatic fall back, switching between normal operation mode and fall back mode is performed by automatic day/night switching via a routing group and not (manually) by a supervisor extension.

1. Create for all required starters a hardware-less extension or Non Member ACD groups (group prop. 45). These extensions/groups are forwarded to a routing group (group prop. 59!).

2. Configure “call forwarding on over flow” to the IVR group.

3. Configure “call forwarding on night” to the agent ACD group.

In normal operation the calls are handled in the IVR group via the “call forwarding on overflow”. When the BCT server is down or cannot be reached, the grouting group will switch automatically to night and the calls will be sent to the agent ACD group via the “call forwarding on night”. The moment BCT is operational again, calls will be sent to the IVR group again. See section 4.5.6.8 Configure Automatic Fall Back for a detailed configuration description.

The following notes are important for **manual** fall back as well as for **automatic** fall back.

Note: *When BCT server is down or cannot be reached, the agents must be present in the ACD groups otherwise they do not receive calls.*

The agent state is synchronized between the switch and BCT during the normal operation mode. The moment the fall back is activated, agents who are ready in BCT will also receive calls when the fall back mode is activated.

There is no Synchronization when the fall back mode is switched back to normal operation mode. This means that the moment the normal operation is active after a period of fall back agents may have an incorrect state. Switching the agent state via the BCT Supervisor Dashboard or agent phone will synchronies the state again.

Note: *When BCT is down and calls are answered via the Fall Back group, there is no reporting on these calls.*

Note: *When BCT is down and calls are answered via Fall Back group, there is no possibility to define “Follow up Actions” or “Call Type” definitions.*

Note: *Agents can be logged in into more than one group in BCT. In the Fall Back Group, agents can only be present in ONE ACD Group.*

4.5.6.7. Configure Manual Fall Back

An example of manual Fall Back configuration is depicted in Figure 4-43 BCT PBX configuration with Fall Back.

The following note is very important and should be communicated clearly to the group supervisor and group agents:

IMPORTANT: *When BCT goes down, the supervisor must activate the Fall Back scenario manually by dialing the Day/Night prefix from the Supervisor extension (here 210). The moment BCT is operational again the supervisor must switch the ACD group to night again.*

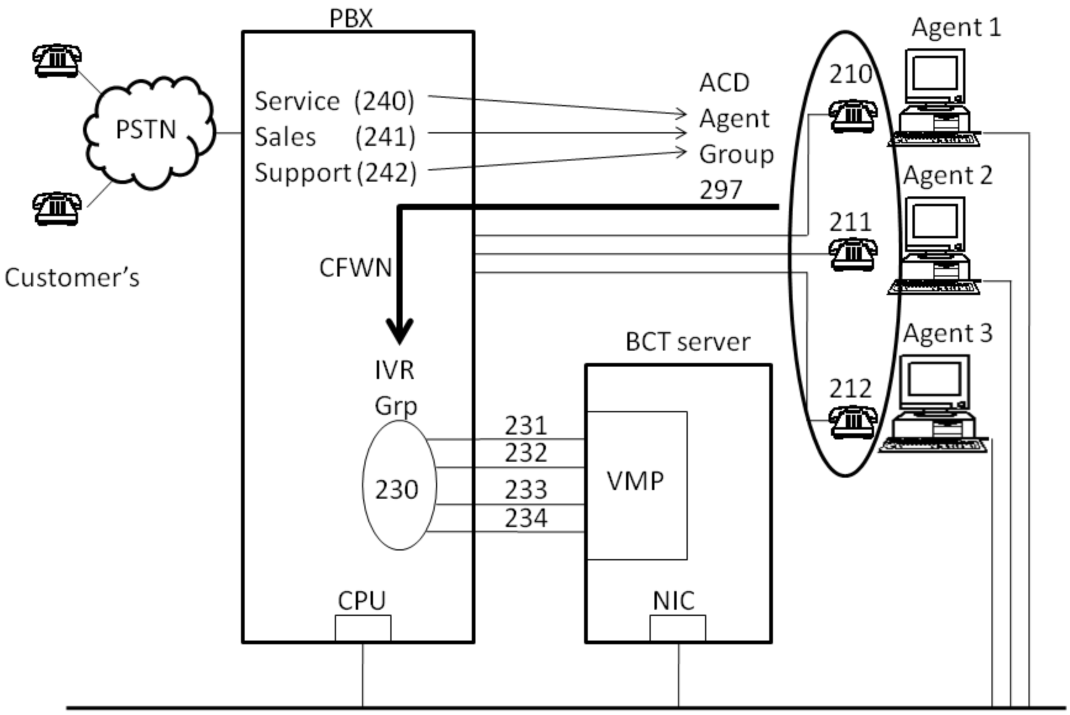


Figure 4-43 BCT PBX configuration with Fall Back

Creating a Hunting Group for the VMP lines

To create a hunting group for the lines to BCT, use the OM command **CRGRPA**. See section 4.5.6.4 PBX configuration for Voicemail for more information.

Creating an ACD Group for Agents

Note: *Do not create a group with a group property that allows any type of call pick-up. Do not use any type of diversion from agent phones, like CFDA, Follow Me, etc.*

Configure an ACD group and assign all agent extensions to that group:

1. Create the agent group using group property 44.

```
CRGRPA:<GROUP DNR>,<GROUP PROPS>;
```

Example:

```
CRGRPA:297,44,,210;
```

In the above listed example, the supervisor is assigned with extension 210.

Always create the ACD agent group with a supervisor, otherwise you cannot switch the group from day to night with a prefix. The only possibility without a supervisor is via an OM terminal.

2. The command asks for the following additional parameters:

```
Unit:; Enter the unit number (only applicable if this system is multi-unit).
ACD group threshold priority:;
Full threshold:;
Busy threshold:;
Forced absent time:;
After call work time:;
Call in queue time:;
Pause tone:;
CallManager MIS logical device ACD:;
Queue Position Algorithm:;
Queue priority of the group:;
```

When the above mentioned information is entered, the system will ask for specific agent information.

```
<Member BSP-ID>,[<SWITCH-ALL>], <RANK>;
```

where: **<Member BSP-ID>** is the extension of the agent.

The **Switch allow/init-status** indicates if an agent is allowed to switch between absent and present. Choose 1, 2 or 3. Do not use 0. In that case the agent is not allowed to switch.

Rank is the unique number in the ACD group.

Example:

```
210,1,0;
211,1,1;
212,1,2;
```

The group that you have created is automatically in “Day” and the members are automatically switched “present” in the group. This is the result of Switch Allowance “1” for the members.

Note: *Switch the agent ACD group to night.*

Night is the normal operation mode when BCT is running correctly. Use OM command:

```
CHGRDN:297,0;
```

where 297 is the agent ACD group and 0 indicates night mode.

If you want to change the ACD configuration use the command:

```
CHACDD:<GROUP-DNR>;
```

If you want to assign more extensions to the group, use command:

```
ASGRPM:<GROUP-DNR>,<Member BSP-ID>,[<SWITCH-ALL>],<RANK>;
```

Assigning Call Forwarding When Night

After you have created the IVR hunting group and the agent ACD Groups, you must setup a “Call Forwarding When Night” from the agent ACD group to the IVR hunting group. Use OM command CHCALF.

Example:

```
CHCALF:5,297,230;
```

Creating prefixes for Fallback

The prefixes for agent switching must be performed with “ACD server dialed” prefixes. In that case the prefixes can also be used for phone based agents.

```
CHCSDD:<TREE>,<NUMBER>,<TRFC><<SERVER_AND_ACTION_CODE>,[,[<PW_NMB_LENGTH>][,<ADD_IN
FO_NBR_LENGTH>]];
```

- **TREE**: Destination tree “0” (initial) and/or “1” (inquiry).
- **NUMBER**: The prefix that agents or supervisor dials for a certain action. These numbers should be “easy” to remember, for example “*31” Agent login and “#31” agent logout.
- **TRFC**: The required traffic class, most of the time the traffic class for agents are low.
- **SERVER_AND_ACTION_CODE**: Server and action codes are used by two types of applications. Message Server and ACD MIS Server. First you have to select for which Server the action is valid. Select 1 (ACD MIS server code) followed by the required action code:
    - 1=Agent logout;
    - 2=Agent not ready;
    - 3=Agent ready;
    - 4=Agent login and ready.
- **PW-NBR-LENGTH**: No password number length must be entered.
- **ADD-INFO-NBR-LENGTH**: The number of digits used for the “not ready reason” and the “call type” should match the number of digits that are used during the creation of these items.

  This parameter defines the number of digits that must be entered for the above mentioned actions. As an example: an agent login is configured with the number “*31” to identify the agent the agent PIN (3-6 digits) must be entered after the “*31” in this example the ADD-INFO-NBR-LENGTH is 3-6.

  The number of digits for the “agent log on and ready” is 3-6 digits.

  The number of digits for “agent not ready” is 1 up to 6 digits. When no “not ready reasons” are required you can omit this value.

  The number of digits used for entering transaction code is 1 up to 6 digits. This prefix is used to enter “call type information”.

Note: *When the prefixes are only used in fall back mode and no phone based agents are used in the Contact Center, “info-nbr-length” value can be ignored.*

Already created prefixes can be displayed with the OM command **DICSDD**.

Prefixes for switch group to night and switch group to day cannot be created with the server dialed prefixes; for these, use OM command ASINTN.

Res. ID	Description
128	ACD Group day prefix
129	ACD group night prefix

Table 4-3 Result identities for group day and group night prefixes

4.5.6.8. Configure Automatic Fall Back

Execute the following steps:

1. Configure an IVR hunting group as described in section 4.5.6.4 PBX configuration for Voicemail.

2. Configure an agent ACD group as described in Creating an ACD Group for Agents.

3. Create agent switch prefixes as described in Creating prefixes for Fallback. There is no need to create the “ACD Group day prefix” and the “ACD group night prefix” these are only used in manual fall back.

4. Create a routing group as described in section 4.5.7.2 Creating a routing group.

   For an automatic fall back it is important that the maximum Queue on the Routing Point is set to zero. This will trigger the “call forwarding on overflow” to the IVR group in normal operation mode. So leave the “busy threshold” and the “full threshold” to the default value of 100% (this is a non member group so the default relative Queue size will be zero).

5. Assign “call forwarding on overflow” to the IVR group.

6. Assign “call forwarding when night” to the agent ACD group.

Note: *Do not forget to configure a Routing Point in BCT. The configured Routing Point will trigger the day and night status of the Routing Point.*

7. For every starter that is required in the Call Flow, create hardware less extensions or non member ACD groups (group prop. 45). Configure “call forwarding on not reachable” to the routing group for the hardware less extensions or configure “call forwarding on night” to the routing group in case you use non member groups.

4.5.7. PBX configuration for Contact Center without IVR

This section explains how to setup the iS3000 PBX for a BCT Contact Center without IVR.

4.5.7.1. General

You can configure a BCT server without IVR. In that case the calls are queued in the PBX. The callers are queued on Routing Points until a free agent is found. In that case the number of available VMP lines is no longer the maximum number of caller that can be queued. When BCT uses Routing Points instead of IVR for queuing it’s called an “IVR-less” system.

A configuration without IVR can’t use the prompt features that are provided by IVR. Only the “in-switch” announcements can be used to inform the callers. The “in-switch” announcements can only be used for a welcome message, night announcement, and Queue status information and not for Call Flow information (attendant, confirmation prompts etc.)

4.5.7.2. Creating a routing group

A routing group is a non member ACD group. The difference between a normal non member group and a routing group is that a routing group can be switched to day and therefore calls will be accepted in the Queue. The routing group is called a Routing Point in the BCT Supervisor Dashboard.

It is possible that more than one routing group is required (multi- language Contact Center, VIP treatments etc.), in that case create as many routing groups as needed. Use the BCT Supervisor Dashboard application to select the correct routing group for the correct Starter Line.

Create of one or more ACD routing groups. Start creating the group with the command **CRGRPA**. The following parameters should be entered.

- **Group-DNR**: Identifies the ACD group. In the BCT Supervisor Dashboard application this is called a Routing Point.
- **Group property**: Enter Group property 59 followed by a semicolon. The system will prompt for additional information.
- **ACD group threshold priority**: Accept the default, threshold priority can be arranged when more than one router is used.
- **Full threshold**: Maximum number of non-threshold and threshold priority calls that can be stored in the ACD Queue.

  The ACD Routing group contains no members and therefore the Full threshold for ACD Routing groups **must** be entered as a fixed value. Enter a value that starts with 99 followed by e.g. 20 (9920) 20 calls in total can be queued. Do not use a value higher than 97.

- **Busy threshold**: Maximum number of threshold priority calls that can be stored in the ACD Queue. Also enter a fixed value, see Full threshold.

  For routing groups used by BCT, it is recommended to use the same value for the busy and full threshold.

  Note: *Do not use a relative Queue for the busy and full threshold for a routing group. This results in a routing group where no calls can be queued.*

  The number of available Queue places should be at least the same as the maximum Queue size that is configured in the Router and the number of callers that can be queued according the granted licenses.

- **Forced absent time**: Accept the default, the forced not ready time is arranged on the router.
- **After call work time**: Accept the default, the after call work time is arranged on the router.
- **Call in queue time**: Calls will be diverted or dropped when the call in queue time has expired. Make sure that the selected call in queue time matches the call in queue time that is set in the router options.
- **Pause tone**: Defines the type of pause tone sent to the caller between announcements.
- CallManager MIS logical device ACD: Not applicable for BCT.
- **Queue Position Algorithm**: Sets the operation mode for the “dynamic delay messages” there are two possibilities Absolute and Weighted.

  In combination with BCT based on IVR-Less, only **Absolute** is supported.

Note: *Be aware that one Routing Point in combination to several starters (one or more Non member groups forwarded to one routing group) will result in incorrect announcements. The iS3000 announcements will play announcements for the Routing Point Queue and not related to the Starter Line router relation. In case of more routers and correct iS3000 announcements per router, more than one Routing Point must be created.*

- **Queue priority of the group**: Select the default value, priority can be arranged in the Call Flow.

Notes:

- These settings can be changed with the CHACDD command.
- The default "COB queue type" is "Short-COB-Queue". For an ACD group the "Short COB Queue" should be changed to "Long-COB-Queue" (CHCOBD). Display the selected "COB queue type" with DICOBD.
- Use OM command ASFACM to assign FCM 47 (overrule CLIR) to the ACD routing group(s).

4.5.7.3. Route settings for free agent check

Per (IVR-Less) Starter Line you can define that the caller to the Contact Center is not connected before a free agent is available. When no free agents are available the PBX must generate busy tone to the caller. This busy tone will only be generated when X (Action when unsuccessful DDI call) in the Tone and DDI options is set correctly.

Use the **CHRTCI** command and check in the parameter **TONE-AND-DDI-OPTIONS** that X (Action when unsuccessful DDI call) is set to zero (busy tone).

4.5.7.4. Call forwarding

The call forwarding destination may be another ACD group but it is also possible to forward to a normal extension or operator extension. For (Skill Based) Routing only Call "Forwarding on group Night service" is applicable (to a Fallback group).

Call Forwarding must be configured with the **CHCALF** command. Displaying Call Forwarding information is possible with the **DICALF** command. The following parameters should be entered:

- **Call forwarding type**: number between 0 and 9.
- **ORIG-BSP-ID**: The groups DNR.
- **DEST-NUMBER**: the destination for this call forwarding.

The following types of call forwarding are applicable for ACD groups:

- Call Forwarding When Absent (CFWA)
  If CFWA is enabled, the call will be routed to another member of the group.
  Call forwarding type for CFWA is 2.

- Call Forwarding on Empty group (CFWE)
  When a call is routed to a group with no members defined (No Member group) or to a group where all the members are switched absent the call will be routed to the destination DNR.
  Call forwarding type for CFWE is 3.

- Call Forwarding on group Overflow (CFWO)
  When a call is routed to an ACD group and all the members of this group are busy and the COB Queue is full, the call will be forwarded to the specified extension.
  Call forwarding type for CFWO is 4.

- Call Forwarding on group Night service (CFWN)
  When a group is switched to “night mode” the calls for this group will be routed to the specified ACD group.
  Call forwarding type for CFWN is 5.

Note: *An ACD group uses the long or short COB-Queue length. The option SYSOP 046 'dynamic group COB with intrusion allowance' is ignored.*

4.5.7.5. Announcements

There are three types of iS3000 announcements:

- **Station call**, first announcement that is given when a customer dials the ACD group extension.

- **Night Announcement**, announcement that is given when the group is in night and the call is diverted to a CFWN destination.

- **Queue Announcement (or delay message)**, a Queue announcement is given when there is no free agent available to accept the call and the call is queued in a COB Queue.

The announcements can be recorded e.g. with the Voice Manager. For information, please refer to the related documents.

4.5.7.6. PBX Configuration with Fall Back scenario

BCT takes over the call distribution from the PBX. If for whatever reason BCT server is down or cannot be reached, all calls will be lost. Therefore it is strongly recommended to configure a Fall Back scenario. There are a number of Fall Back options possible.

Creating Automatic Fall Back

When BCT uses routing groups, automatic fall back can be configured.

When the Contact Center is running in normal mode, the routing groups are in Day status. Calls are accepted in the Queue and BCT routes the calls to agents.

When the BCT server is down or cannot be reached any more, the routing groups automatically switch to night mode. Via a call forwarding when night, the calls are routed to an ACD fall back group.

This ACD group must contain all agents that are working in the Contact Center, and must always be in day mode. And the ACD group extension should not be announced to the callers of the Contact Center.

Notes:

- When BCT is operational, the status of the agents are synchronized with the PBX. When BCT switches over to the Fallback configuration the agents already have the correct status. From that moment on the agents must use the login/logout prefixes that are created in the PBX to switch status.

- When BCT is functioning again, the agent status in the PBX may be out of sync with the status of the agents in BCT (when BCT is down the status of the agents cannot be updated).

- When BCT is down and calls are answered via the Fall Back group, there is NO reporting on these calls.

- When BCT is down and calls are answered via Fall Back group, there is NO possibility to define "Follow up Actions" or "Call Type" definitions.
- Agents can be logged in into more than one group in BCT. In the Fall Back Group, agents can only be present in ONE ACD Group).

Creating an ACD Fall Back Group

An ACD fall back group is a normal ACD group.
Create the group with the command **CRGRPA**. The following parameters should be used:

- **Group-DNR**: Identifies the ACD group. This extension is used as destination for call forwarding when night during the fall back period.

- **Group property**: See the OM commands manual for an overview of the available group properties. The value must be between 30 and 45.

  Some examples:

  Group property 36:
  - Longest idle hunting,
  - call pickup group and member allowed,
  - empty group not allowed.

  Group property 45:
  - Longest idle hunting,
  - call pickup group and member allowed,
  - empty group allowed.

  Enter the appropriate group property value. The system will prompt for additional information.

- ACD group threshold priority:
  Accept the default. This is only applicable if a second ACD group is used as destination in a call forwarding.

- **Full threshold**: Maximum number of non-threshold and threshold priority calls that can be stored in the ACD Queue.

- **Busy threshold**: Maximum number of threshold priority calls that can be stored in the ACD Queue. Also enter a fixed value, see Full threshold.

  Note: *For an ACD fall back group used by BCT, it is recommended to use the same value for the busy and full threshold. The size of the threshold should be equal to the Queue size that is used in the router settings.*

- **Forced absent time**: When a call is not answered within this time, the agent will be switched absent and will not receive ACD calls any more.
  Use the same duration as used in the router.

- **After call work time**: After an ACD call is finished, the agent will not receive another call within this time frame. Use the same duration as used in the router.

- **Call in queue time**: Calls will be diverted or dropped when the call in queue time has expired. Make sure that the selected call in queue time matches the call in queue time that is set in the router options.
- **Pause tone**: Defines the type of pause tone sent to the caller between announcements.
- CallManager MIS logical device ACD: Not applicable for BCT.
- **Queue Position Algorithm**: Sets the operation mode for the “dynamic delay messages” there are two possibilities Absolute and Weighted.

Concerning the Queue Position Algorithm, two types of announcement are important, Static Delay Message (SDM) and Dynamic Delay Massage (DDM).

If **absolute** is selected, DDM is related to the Queue position.

In the following example, three DDM messages are defined.

Queue position	Played announcement	
1	DDM 1	“You are the next in line”
2	DDM 2	“There is one waiting call”
3	DDM 3	“There are two waiting calls”

When **weighted** (also called relative) is selected the following formula is applicable.

$$\mathrm{DDM} = \left(\left(\frac{\text{Queue position -1}}{\text{Number of present agents} \times \text{Full theshold}} \right) \times \text{Max. Number of dynamic delay announcements} \right) +1$$

In the following example the weighted method is used with three Dynamic Delay Messages and the full threshold of 2 per agent.

– **Queue position**	– **Played announcement for ..... present agents**			
	– **4**	– **3**	– **2**	– **1**
– 1	– DDM1	– DDM1	– DDM1	– DDM1
– 2	– DDM1	– DDM1	– DDM1	– DDM2
– 3	– DDM1	– DDM1	– DDM2	–
– 4	– DDM2	– DDM2	– DDM3	–
– 5	– DDM2	– DDM3	–	–
– 6	– DDM2	– DDM3	–	–
– More than 6	– DDM3	–	–	–

Table 4-4 Queue position - Announcement table

- **Queue priority of the group**: Used to give one ACD group a higher priority than another group. Select the default value, priority is only applicable when a next ACD group destination is configured.

  When the above mentioned information is entered, the system will ask for specific agent information.

- **Member BSP-ID**: DNR of the agent.

- **Switch allow/init-status**: There are 4 switch allow/init-state possibilities:

  Switch allow/init-state: 0 Not allowed to switch status. Initial state: logged in and present.

  Switch allow/init-state: 1 Allowed to switch status. Initial state: logged in and present.

  Switch allow/init-state: 2 Allowed to switch status. Initial state: logged in and absent.

  Switch allow/init-state: 3 Allowed to switch status. Initial state: logged out and absent.

  The init-state is the status of the agents after the ACD group is created and after warm or cold start of the PBX.

  Option 0 will not be used in Contact Centers, agents are not able to switch status during the fall back period. Recommended is switch allow/init-status 1. The result will be that the moment the fall back is activated all agents are logged in and ready to answer calls.

  Be aware that is possible that a number of agents are not at their desk but the telephone is ready to receive calls. These calls will be rerouted (after a forced not ready) to agents that are available. You also may consider using switch allow/init-status 1 for a number of agent's extensions that are used more frequently than other agent seats, and that the remaining agent's extensions will be created with switch allow/init-status 3. This to avoid that callers are waiting a long time due to rerouting on forced not ready.

  This is only a problem for screen based agents. When the Contact Center is using phone based agents, the status of the agent will not be changed the moment the fall back is activated.

- **Rank**: Unique number used for cyclic hunting.

  Enter for each agent that is working in the Contact Center an extension and a rank. The rank is a unique number within an ACD group. When all agents are entered, end the command with return. At this moment the ACD group is created.

  Note: *The default "COB queue type" is "Short-COB-Queue". For an ACD group the "Short COB Queue" should be changed to "Long-COB-Queue" (CHCOBD). Display the selected "COB queue type" with DICOBD.*

4.5.7.7. Assigning call forwarding when night

After you have created one or more routing groups and the ACD fallback groups, you must setup a "Call Forwarding When Night" from the routing group(s) to the ACD fallback group.

Use OM command CHCALF. Example:

```
CHCALF:5,<routing group>,<ACD fall back group>;
```

Execute this command for each routing group that is created.

4.5.8. Company Directory and Presence Information on Polycom terminals

Polycom terminal users can access the Company (or Central) Directory to search for an entry, look at the presence information and set up a call.

To allow this, you must modify the sip.cfg configuration file of the terminal so it will point to the BCT server as server application. Please refer to the “SIP in iS3000 – Customer Engineer Manual” [on the iS3000 Documentation CD-ROM] for more information.

To allow an application to be run from the microbrowser:

1. Open the sip.cfg configuration file in an XML editor.
   You can find this file on the TFTP server in the LAN network.

2. Locate the Microbrowser <mb> parameter.

3. Optional: change mb.proxy to the address of the desired HTTP proxy to be used by the Microbrowser.

For example:
mb.proxy=10.11.32.103:8080 where 10.11.32.103 is proxy server IP address and 8080 is the port number.

4. Change mb.idleDisplay.home to the URL used for Microbrowser idle display home page.

For example:
mb.idleDisplay.home=http://10.11.32.103:8080/sampleapps/idle

5. Change mb.idleDisplay.refresh to the period in seconds between refreshes of the idle display Microbrowser’s content.

For example:
mb.idleDisplay.refresh=10

6. Change mb.main.home to the URL used for microbrowser home page.

For example:

```
mb.main.home=http://<ServerName>/HtmlDirectory/Default.aspx?type=directory
```

where ServerName is either the server name string or, if you have executed step 3, the proxy server IP address and port number.

7. Change mb.limits.node to the maximum number of tags that the XML parser will handle.

For example:
mb.limits.nodes=256

8. Change mb.limits.cache to the maximum total size of objects downloaded for each page (both XHTML and images).

For example:
mb.limits.cache=200

The application which enables Polycom terminals to search the directory is called “HTML Directory” and can be found on: “C:\Inetpub\wwwroot\HTML Directory”.

When open the Configuration Manager and select the configuration file “C:\Inetpub\wwwroot\HTML Directory\web.config file” for this application then you can configure the result page for a search query by means of changing the value of the keys.

Keys description:

- maximumDataInPage: maximum number of entries shown in one page. Default value: 4
- showPhoneState: show 'Phone State' icon for each entry. Default value: False
- showDetails: show 'Details' icon for each entry. Default value: True

When “showPhoneState” is changed to “true” the DataAccess.dll.config has to be changed also:

- Open the file DataAccess.dll.config with Notepad. Default location: C:\Program Files (x86)\Common Files\NEC\Services directory.

  Note: *When the system was upgraded the location path is C:\Program Files (x86)\Common Files\Philips\Services.*
- Find the key “directory.service.presence.algortithm” and set its value to “BCTOnly”.
- Save the file.
- Reboot the server.

The used language on the Polycom directory browser is the same as the BCT system language.

4.5.9. iS3000 configuration for Mobile Clients

A mobile extension is a Mobile phone or other external phone that can act as a local extension in the iS3000. When the Mobile smart phone which is related to the mobile extension is capable of browsing to the BCT server, it can login with the BCT Mobile Client application and use several BCT functions like Directory Access and Presence Management.

In iS3000 the mobile extension is Mobility Access. With this functionality a remote extension (e.g. Mobile phone) can be reached under a local extension number and can use the same features as a local extension, like consultation call, transfer (consultation and blind) and conference. To program the MA, execute the following procedure:

1. Assign a PM shelf with type 17 “Virtual MA shelf” with command:

```
ASSHLF: <SHELF>, <Shelf-type>;    with Shelf-type = 17 for Virtual MA shelf
```

2. Assign a PMC-board at position 17 in the newly created SMA shelf with command:

```
ASBRDS:<SHELF>,17,90,0201,225,0;   for CCS
ASBRDS:<SHELF>,17,91,0201,225,0;   for CPU3000, CPU4000
```

3. Assign a PCT-board of type 38 “Virtual MA board” in the newly created SMA shelf with command:

```
ASBRDS:<SHELF>,<BOARD>,38,0201,255,1;
```

4. Set the PMC-board and PCT boards and circuits in service with command

```
SETINS:<SHELF>,<BOARD>,<CIRCUIT>;
```

5. Assign the mobile extension number to a circuit of the PCT board with command:

```
CHSMAR: <SHELF>,<BOARD>,<CIRCUIT>,<Dest-Number>;
```

with the Dest-Number consisting of the TAC and the telephone number of the mobile extension

6. Assign a local extension to the PCT board with command:

```
CHDNRC:<LocalDNR>,<SHELF>,<BOARD>,<CIRCUIT>;
```

with the LocalDNR as the DNR known in BCT

Further information can be found in iS3000 manual “Networking & Routing Facilities - Explained”, chapter ”How to Program SMA”.

Note: *With MA it is possible to activate/deactivate the local DNR on the remote/local terminals. Because BCT cannot recognize the (de-) activation of the local DNR this feature not supported. Instead, only Fixed SMA is supported where a System Engineer activates the MA. After activation a PBX Synchronization in BCT is required to recognize the MA extensions.*

4.5.10. Configuration for Bria softphone support

Bria is a softphone that can be used as telephone for BCT uses. To control the softphone via BCT Desktop Client interface, the Bria softphone and extensions need to be configured.

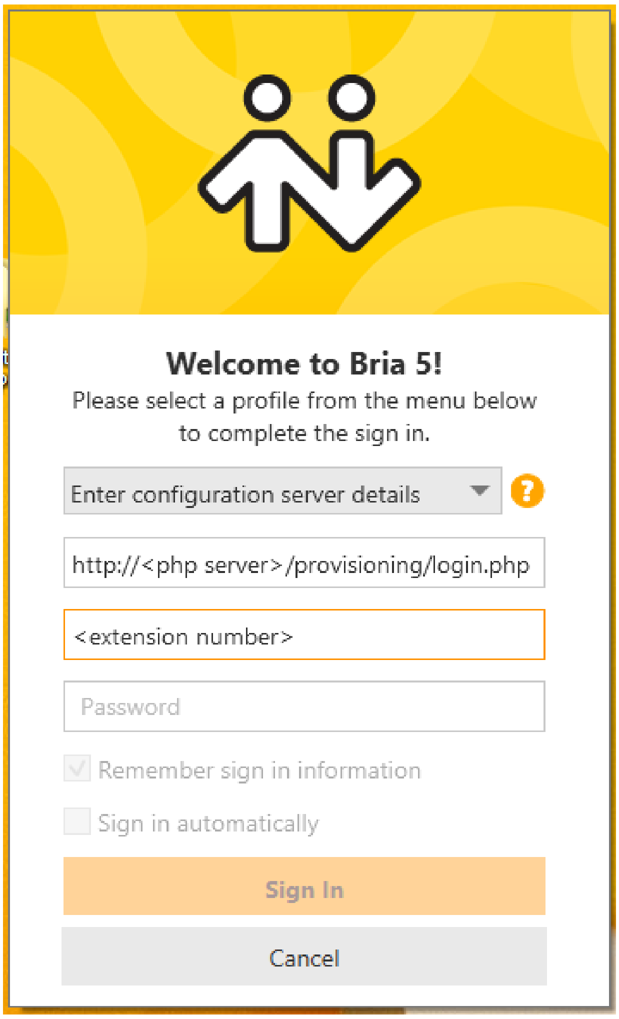
The Bria version 5 can get its configuration settings from a Login server. This Login server is a PHP server that contains a login script that the Bria phone retrieves during startup.
After configuring the PHP server, a login script should be created to configure the Bria.

An example for the login.php script:

```
<?php
//
//
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
$user = $_POST['Username'];
$display_name = $_POST['Username'];
$passwd = $_POST['Password'];
} else {
$user = $_GET['Username'];
$display_name = $_GET['Username'];
$passwd = $_GET['Password'];
}
$domain = "172.16.67.11";
$response =
"[Data]
Success=1
[Settings]
proxies:proxy0:display_name=\"$display_name\"
proxies:proxy0:username=\"$user\"
proxies:proxy0:password=\"$passwd\"
proxies:proxy0:authorization_username=\"$user\"
proxies:proxy0:domain=\"$domain\"
proxies:proxy0:account_name=\"BCTPhone\"
proxies:proxy0:register=\"1\"
proxies:proxy0:enabled=\"1\"
```

```
proxies:proxy0:enabled_features=\"-1\"
proxies:proxy0:use_sip_call_info_to_force_offhook =\"1\"
system:remote_control:enable_talk =\"1\"
system:remote_control:enable_hold =\"1\"
proxies:proxy0:send_sip_keep_alive_messages=\"0\"
proxies:proxy0:firewall_traversal_mode=\"0\"
proxies:proxy0:subscribe_to_message_waiting=\"0\"
proxies:proxy0:enable_features=\"03\"
codecs:g711a:enabled=\"1\"
codecs:g711u:enabled=\"1\"
codecs:g722:enabled=\"0\"
codecs:g729:enabled=\"0\"
codecs:h263:enabled=\"1\"
codecs:h263_1998:enabled=\"0\"
codecs:h264_unified:enabled=\"0\"
codecs:silk_nb:enabled=\"0\"
codecs:silk_swb:enabled=\"0\"
codecs:silk_wb:enabled=\"0\"
codecs:speex:enabled=\"0\"
codecs:speex_fec:enabled=\"0\"
codecs:gsm:enabled=\"0\"
codecs:speex_wb:enabled=\"0\"
codecs:speex_wb_fec:enabled=\"0\"
codecs:vp8:enabled=\"0\"
codecs:amr-wb:enabled=\"0\"
codecs:opus:enabled=\"0\"
rtp:inactivity:timer_enabled=\"0\"
";
print $response;
?>
```

When the Bria softphone is started then Login should be entered:



Welcome to Bria 5!

Please select a profile from the menu below to complete the sign in.

Enter configuration server details

http://<php server>/provisioning/login.php

<extension number>

Password

☑ Remember sign in information

□ Sign in automatically

Figure 4-44 Bria login screen

The terminal type of a Bria extension is initially synchronized as SIP, which lacks the enhanced functionalities in the Desktop client. To use the enhanced functionality, the terminal type of the Bria extensions should be overruled with type Polycom/DT700/DT800/DT900.

To configure this, use the following procedure:

1. Open the Company directory tab of the BCT System Settings.
2. Select Extension searching and search for the Bria extension and open it with Edit
3. Find the field **Manual Terminal Type** and select Polycom/DT700/DT800/DT900 from the drop-down list
4. Press **Apply** to confirm the changes.

4.5.11. Configuration for redundant SIP@Net system

In a redundant SIP@Net system there are one or more active SIP@Net servers and one or more standby SIP@Net servers. BCT must be connected to an active SIP@Net server.
BCT supports failover to an active SIP@Net server when the connected server fails or becomes standby.

BCT supports the following redundant SIP@Net configurations:

- SIP@Net Dual Server LAN.
  To the outside world this configuration acts as a single SIP@Net server.
  There is no need for failover by BCT.
- SIP@Net Dual Server WAN.
  There are two Master servers in the SIP@Net configuration, one is active and the other one is standby.
  When the PBX swaps the active server and the standby server, BCT follows with a failover to the new active server.
- SIP@Net Server Cluster.
  There is one Master server and one or more Slave servers in the SIP@Net configuration. Normally the Master server is active but when the Master server fails the Slave servers become active.
  When the Master server fails BCT can failover to one of the Slave servers. When the Master server becomes active again BCT will failback to the Master server.

Switching a SIP@Net server to active or standby will never be initiated from the BCT application. The SIP@Net system determines which servers are active, BCT follows by connecting to an active server.

Alarms are generated during automatic failover or when a failover fails. Other significant events are logged as system status events, see 11.2.1.2 System Status.

To configure a redundant SIP@Net system in BCT, see 8.6 Configuring redundant PBX configurations.

4.5.12. Call Recording

4.5.12.1. User-initiated Call Recording

BCT operators, agents and Employees can record a call. To make this work you must assign 'Add-on entitled' to the DNRs of all BCT users who are entitled:
ASFACM:0,<DNR>;

Note: this is only required for call recording initiated by the BCT user using his Desktop Client.

4.5.12.2. PBX Configuration for SIP@Net Call Recording

In a SIP@Net system that supports the feature "call recording by SIP@net", you need to execute the following commands to configure properly call recording by SIP@Net:

1. Call recording settings can be changed when installing (or repairing) the settings for the SIP@Net media-server. On one of the settings-pages you can specify the location to store call recordings. Be sure directory-structure is set to 'flat'.

2. System option 222 (extended filename-format for voicerecording) must be set to true. (See 4.5.3 Boundaries, options and licenses).

3. Assign Facility 87 (Voice Recording) or Facility 94 (Voice Recording Conditional) for extensions that you want to use recording: ASFACM:87,<ext-dnr>; or ASFACM:94,<ext-dnr>;
   It is also possible to assign Facility 94 (Voice Recording Conditional) on a Routing point to create recording during routed calls to agent extensions.

4. Define in PBX Configuration the Call Recording Location (see 8.1.5 Connection to PBX).

4.6. BCT on UNIVERGE 3C

4.6.1. Introduction

Chapter 4.6 BCT on UNIVERGE 3C serves as a step-by-step guide, which will show you how to install and configure BCT in a UNIVERGE 3C environment. This chapter is designed to walk the reader through the installation and configuration from beginning to end in sequential order. It is strongly advised to follow this chapter in order and not "skip ahead" as some installation steps are required to be completed before other steps are started. Chapter 24 Appendices N – BCT ON UNIVERGE 3C CONFIGURATION DETAILS describes a number of UNIVERGE 3C configuration details.

Throughout this guide, the diagrams shown in 4.6.1.4 Operator configuration and 4.6.1.5 Call Center configuration will be used as examples during the configuration process. Please note that these diagrams are only example configurations and do not show every possible configuration which can be set in BCT.

Prerequisites

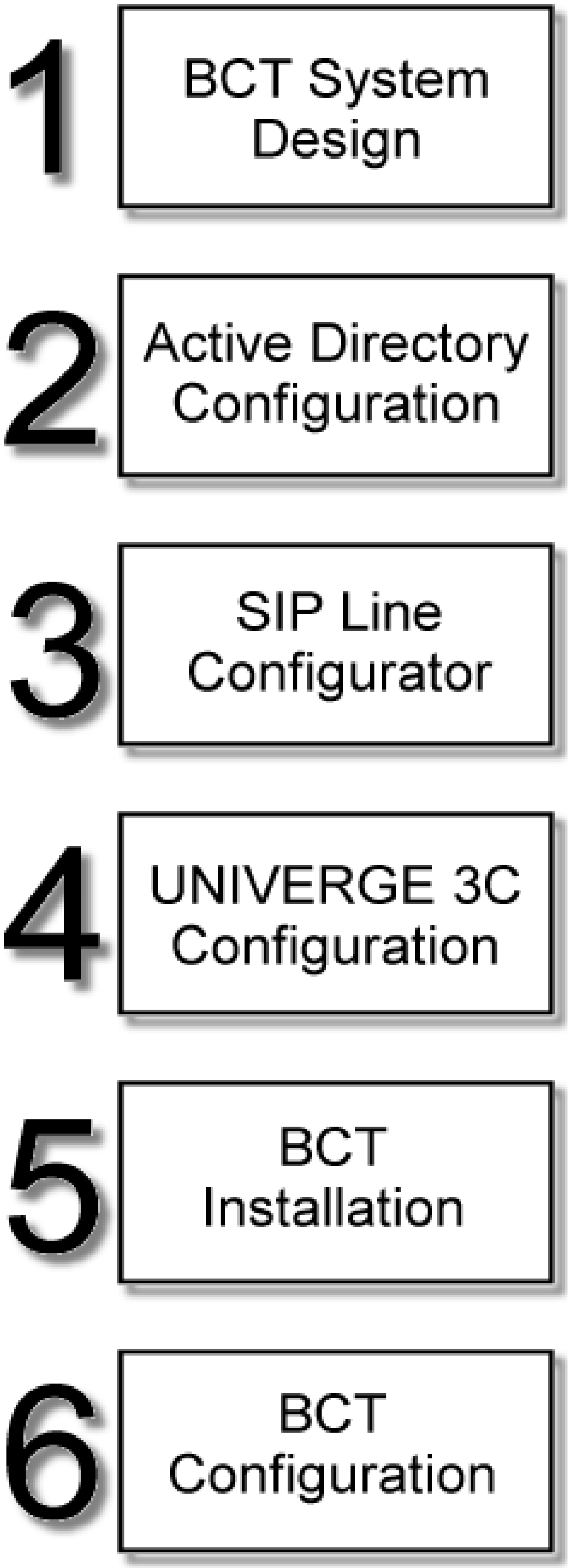
Before you attempt to install BCT refer to prerequisites found in:

BCT Boundary Specification	Most hardware and software requirements will be found here.
BCT Installation Guide	Chapter 2 SYSTEM REQUIREMENTS

Additionally, this guide assumes that:

- Active Directory is installed and is working.
- SQL Server (if it is to be used) is installed and working. A database instance needs to be created for BCT use before BCT is installed. See section 6.1 Database Installation.
- The UNIVERGE 3C is installed and is working (station-to-station calling, station-to-trunk calling, trunk-to-station calling, etc.).
- The computer on which BCT will be installed has a working Operating System (with current service packs and updates) which is supported according to the BCT Boundary Specification document.
- The computer on which BCT will be installed has been joined to the same Domain as the UNIVERGE 3C server.
- The computer on which BCT will be installed has been assigned a static IP address.

4.6.1.1. BCT with UNIVERGE 3C Installation Flowchart



See: 4.6.1.3 BCT System Design

Before you begin, define what needs to be setup for your BCT system**.** This will include station numbers, server IP addresses, call flowcharts, etc.

See: 4.6.2 Active Directory

Create the CTIuser account in Active Directory. This account is used by BCT for a variety of functions.

See: 4.6.3 UNIVERGE 3C SIP Line Configurator

The UNIVERGE 3C SIP Line Configurator is a tool which is included with the BCT installation software (DVD or download) and is used to create SIP extensions for use by BCT.

See: 4.6.4 UNIVERGE 3C configuration

Modify UNIVERGE 3C system settings. Add and modify stations, extensions, and users for use with BCT.

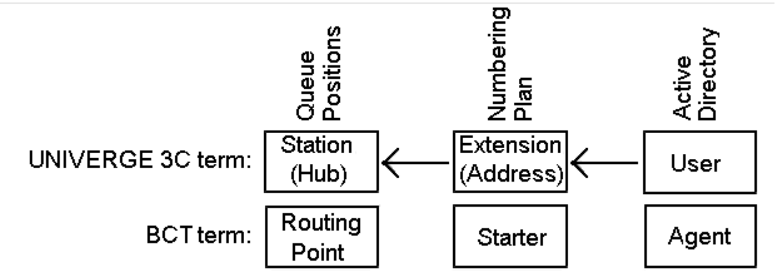
See: 4.6.5 Business ConneCT installation

Install the BCT prerequisites and BCT software. Run an initial synchronization with UNIVERGE 3C and Active Directory using the BCT Configuration Wizard.

See: 8 SERVER CONFIGURATION

Configure BCT Operator and Contact Center call flows.

4.6.1.2. Terminology used



User/Agent: Simple Definition – The person using the terminal and/or client to answer and initiate calls.

Terminology – This person is called a User in the UNIVERGE 3C and an Agent in BCT.

Description –An Active Directory User account is imported into UNIVERGE 3C and attached to one or more Extensions.

Extension/Starter: Simple Definition – The number that is dialed to reach a party or destination.

Terminology – In the UNIVERGE 3C this number is called an Extension or Address. In BCT it is called a Starter. However, it should be noted that while all Starters are Extensions, not all Extensions are Starters.

Description – One or more extensions are attached to a Station. Extensions take numbers from the Numbering Plan.

Station/Routing Point: Simple Definition – That which is receiving or initiating calls (terminal, soft phone, virtual number, or monitored number).

Terminology – In the UNIVERGE 3C this is called a Station or Hub. In the BCT, it is called a Routing Point. However, it should be noted that while all Routing Points are Stations, not all Stations are Routing Points.

Description – The Station contains the address where a call will originate or be delivered (e.g. MAC address of a physical terminal). In regards to BCT, the Station also determines how many queue positions are available (maximum 200).

Messagebox: In this chapter, the term “Messagebox” means the same thing as “Voicemail”.

User centric: More than 1 extension may be assigned to the user.

Address centric: Only 1 extension may be assigned to the user.

4.6.1.3. BCT System Design

Before you install BCT, you need to decide what numbers (Stations and Extensions) will need to be allocated from the Numbering Plan. In some cases the Extension number will be the same as the Station, in others both Extension and Station will need to be unique.

The chart below will help you determine what numbers you will need to allocate during the installation as well as showing what licenses are required.

Note: For UNIVERGE 3C and multiple BCT servers, see also: *8.1.3.2.1 PBX-based License*

Numbering Plan	Required Licenses

	Station	Extension	BCT	3C[1]
CTIUser	None	Unique[2]	None	1 User License
Operator				
External Pilot	Unique	Same as Sta.	None	1 Station License
Internal Pilot	Unique	Same as Sta.	None	1 Station License
Failover Pilot	Unique	Same as Sta.	None	1 Station License
Park Pilot	Unique	Same as Sta.	None	1 Station License
System Call Park	Unique	Same as Sta.	None	1 Station License
Operators	Unique	Same as Sta.	1 Operator License per Operator (Dynamic)[3]	1 User[7] + 1 Station License per Operator
Supervisors[4]	Unique	Same as Sta.	1 Operator + 1 Supervisor License per Supervisor (Dynamic)	1 User[7] + 1 Station License per operator
Contact Center				
Pilot	Unique	Same as Sta.	None	None (only 1 Station License on the routing point required)
Agent Log-on[5]	None	Unique	None	None (only 1 Station License on the routing point required)
Messagebox Access	None	Unique	None	None (only 1 Station License on the routing point required)
Prompt Recording	None	Unique	None	None (only 1 Station License on the routing point required)
Agents	Unique	Same as Sta.	1 Agent or 1 Phone Only Agent License per Agent (Dynamic)	1 User[7] + 1 Station License per Agent
Supervisors[4]	Unique	Same as Sta.	1 Operator and/or Agent + 1 Supervisor License per Supervisor (Dynamic)	1 User[7] + 1 Station License per operator
VMP/IVR				
Hunt Pilot	None	Unique	None	None
Lines[6]	Unique	Same as Sta.	1 VMP License per Line (to a maximum of 200)	1 Station License per Line

Note 1: *A 3C Station License is also known as an STL and a User License is also known as a UAL.*

Note 2: *The Extension associated with the CTIuser account will never receive or originate calls so any number may be used.*

Note 3: *A Dynamic License means that it is only used when a device is logged in. For example, if you have 2 Operator Licenses, you can still assign 3 or more Operators in the system but only 2 Operators may be logged in at the same time.*

Note 4: *A Supervisor must also be assigned as an Operator and/or Contact Center Agent even if they will never take calls.*

Note 5: *This is used by Phone-Only Agents (meaning they do not use the BCT Client) for logging into BCT. If Phone-Only Agents are not used, this number is not required.*

Note 6: *The number of required VMP lines depends on how many callers will simultaneously be able to hear prompts or music on hold. For example: if there are 20 callers listening to music on hold, 15 listening to a queue prompt ("thank you for holding"), and 3 listening to a messagebox, then you will need 38 VMP lines.*

Note 7: *The User license for Operator, Agent or Supervisor is only required if they want to perform IM with 3C UC Client or wants to use a 3C UC Client.*

Other licenses which apply to BCT are shown in the chart below.

	Numbering Plan		Required Licenses	
	Station	**Extension**	**BCT**	**3C**
Other General BCT Licenses				
BCT Basic Service	None	None	1 BCT License per System	None
Additional Languages	None	None	1 Language License per additional Language	None
Other Operator/Contact Center Licenses				
Auto Attendant	None	None	1 Auto Attendant License per System	None
Call Recording	None	None	1 Call Recording License per System	None
Customer Identification Routing	None	None	1 Cust. ID Routing License per System	None
Outbound Services	None	None	1 Outbound Services License per System	None
Skill Based Routing	None	None	1 Skill Based Routing License per System	None
Supervisor Reports	None	None	1 Sup. Reports License per System	None
Voicemail Only User	Unique	Same as Sta.	1 VM License per user	1 User License + 1 Station License per user
Soft Wallboards	None	None	1 Soft Wallboard License per Wallboard (to a maximum of 64)	None
Post Call Survey	None	None	1 Survey License per System	None
Other Integration Licenses				
3rd Party Applications	None	None	1 Application Integration License per System	None
Microsoft Outlook Calendar	None	None	1 Calendar Integration License per System	None
Voicemail to Email	None	None	1 VM to Email Integration License per System	None
EMEA Only Licenses (Not used for North America)				
Employee	Unique	Same as Sta.	1 Employee License per user	1 User License + 1 Station License per user
Hard Wallboard	None	None	1 Hard Wallboard License per Wallboard	None

4.6.1.4. Operator configuration

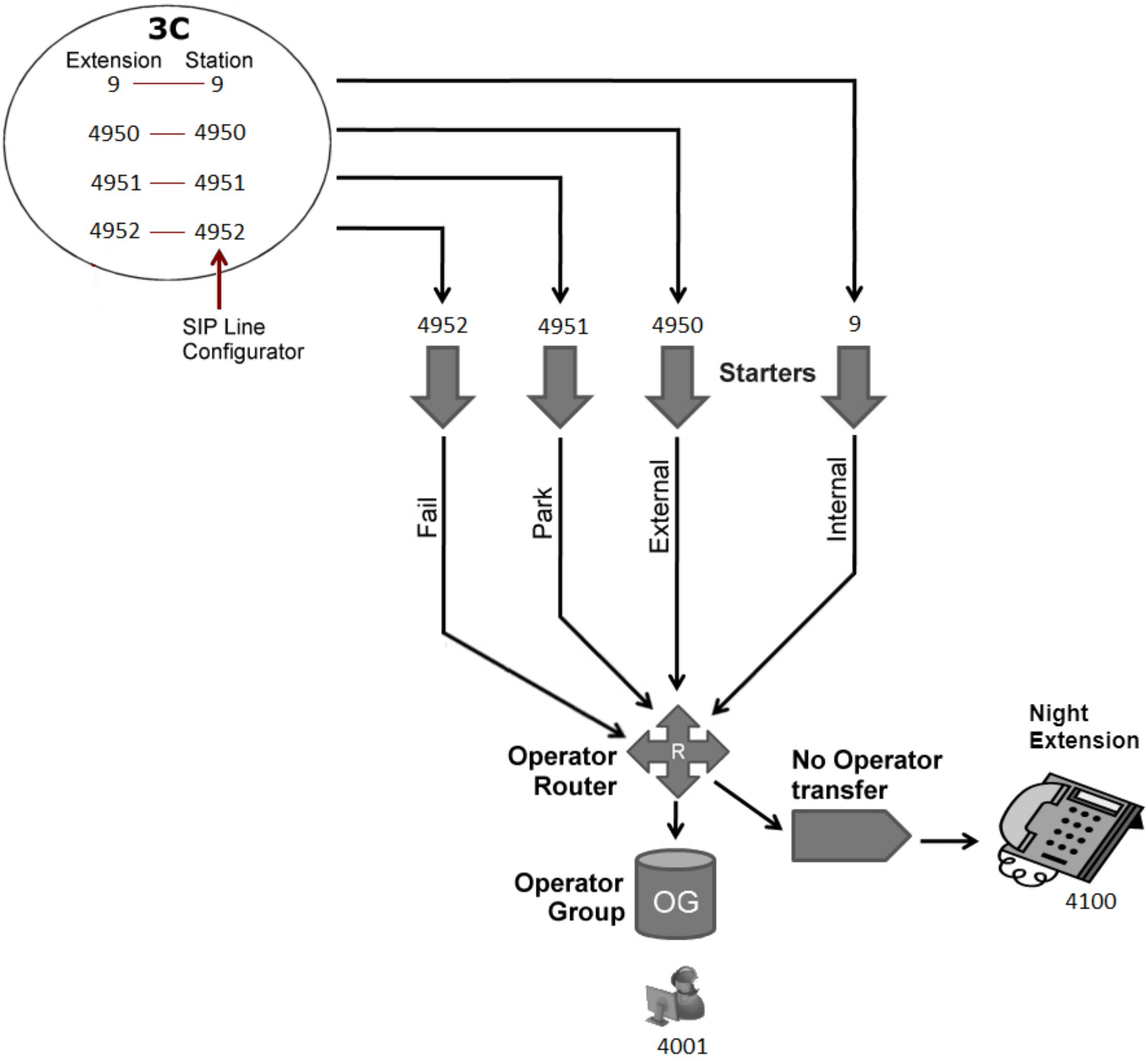


Figure 4-45 Operator Configuration

4.6.1.5. Call Center configuration

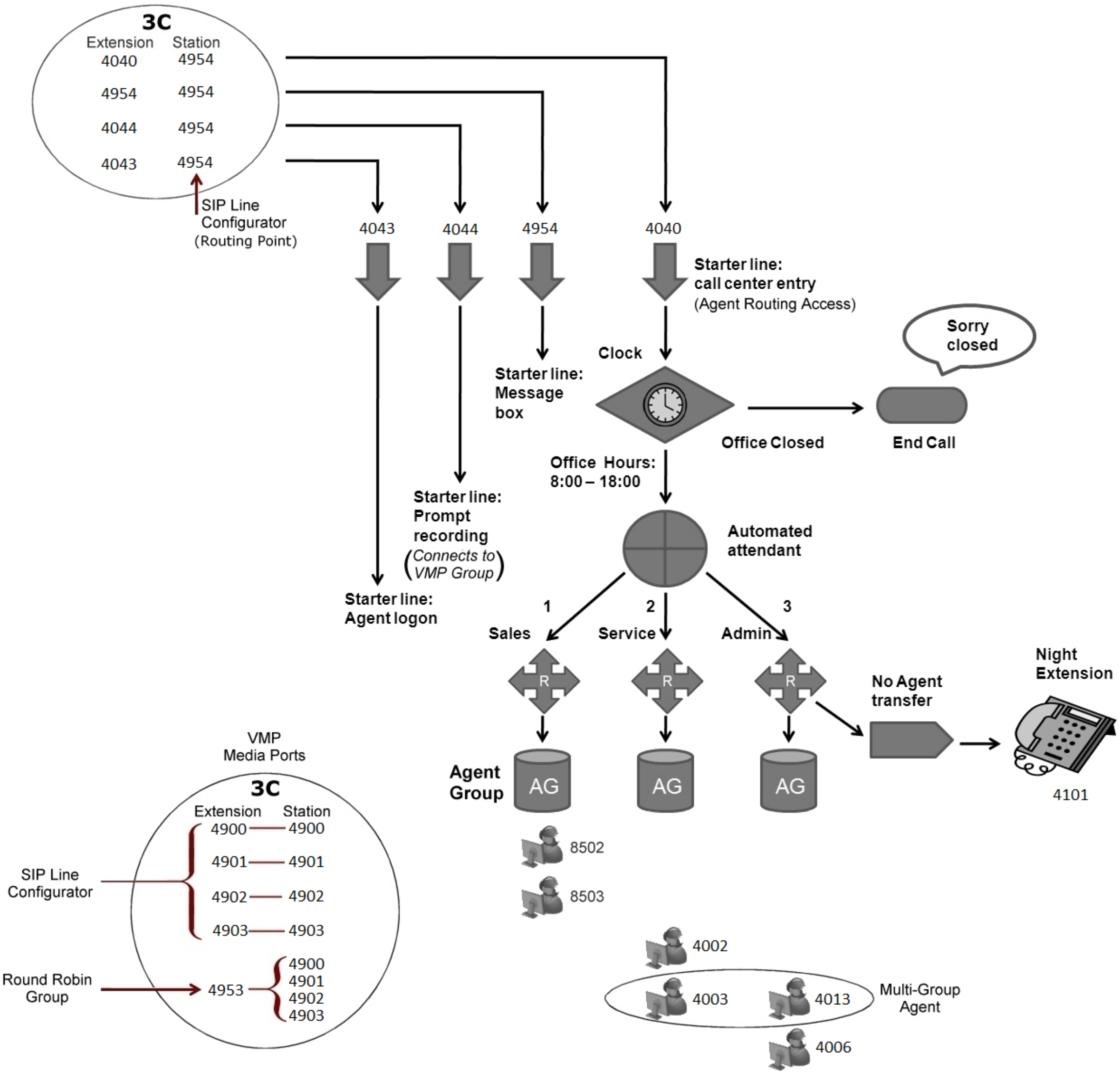


Figure 4-46 Call Center Configuration

4.6.2. Active Directory

A **CTIuser** account is mandatory to be created, for several reasons. This account is, amongst others, used for presence monitoring, call control and Active Directory Synchronization of BCT users.

In order to create this user you must be logged in on the domain controller with an account that has domain administrator rights. If you do not have an account with these rights yourself, then you should have this procedure being performed by an IT administrator.

Note: *for more information about Active Directory see Appendix N-5 – Active Directory synchronization.*

4.6.2.1. How to create a CTIuser account

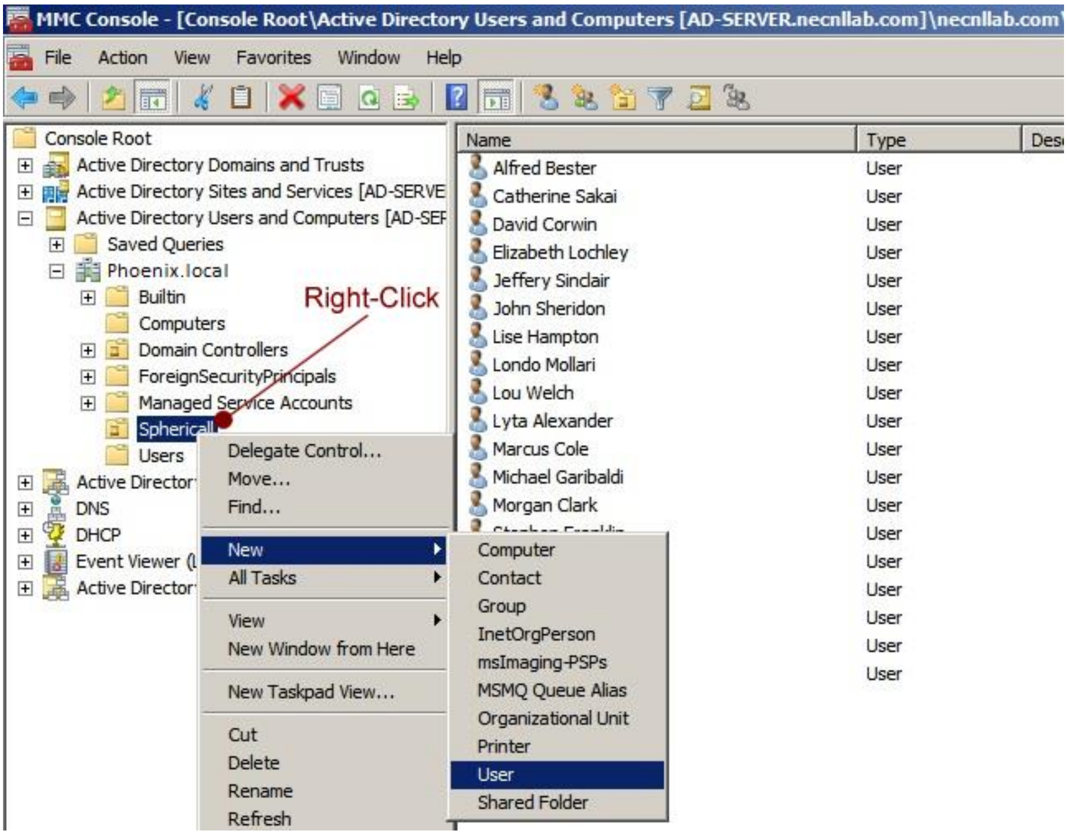
Note: *in this example the user "CTIuser" is created, you do not necessarily need to name this account this way, it is just an example which will be used throughout the manual.*

Note: *CTIuser will be a member of the Domain Users only.*

1. Login on a domain controller of your domain, with an account that is a member of the “Domain Admins” group.

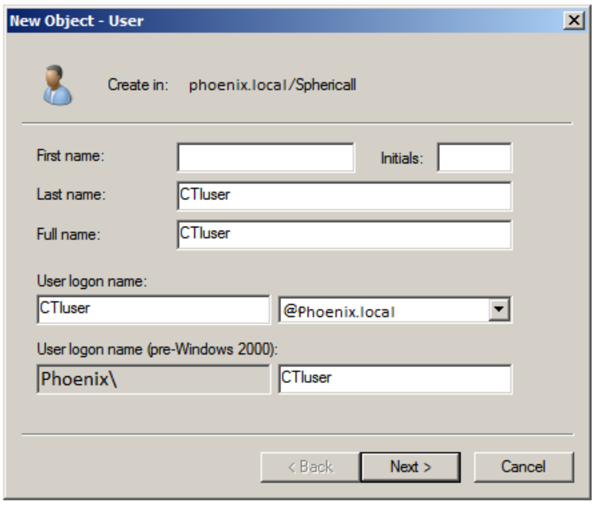
2. Go to **Start > All Programs > Administrative tools** and click the **Active Directory Users and Computers** snap-in.

Right-click the Organizational Unit or AD container (example; the Sphere container) where you want to add the CTIuser account and select **New** and then **User**.



3. In the **New Object – User** window, enter the following and then click **Next**;

First name: Leave blank
Initials: Leave blank
Last name: Enter "CTIuser"
Full name: Leave default, this will be filled in automatically
User logon name: Enter "CTIuser" and choose the domain from the pull down menu
User logon name (pre-Windows 2000): Leave default, this will be filled in automatically



New Object - User

Create in: phoenix.local/Sphericall

First name:

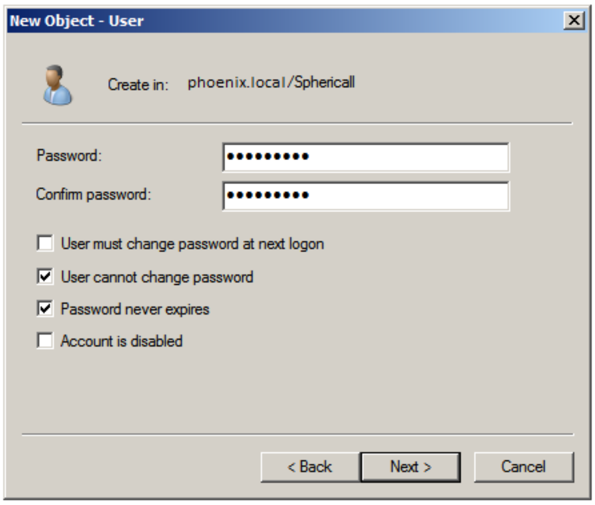
Initials:

Last name: CTIuser

Full name: CTIuser

User logon name: CTIuser @Phoenix.local

User logon name (pre-Windows 2000): Phoenix\ CTIuser



New Object - User

Create in: phoenix.local/Sphericall

Password: •••••••••

Confirm password: •••••••••

☐ User must change password at next logon

☑ User cannot change password

☑ Password never expires

☐ Account is disabled

Note: *The domain phoenix.local.com is just an example, in your case it will be a different name.*

Create a strong password and clear the "User must change password at next logon" checkbox. Select the "User cannot change password" and "Password never expires" checkboxes and click **Next**.

4. Review your settings and press Finish.

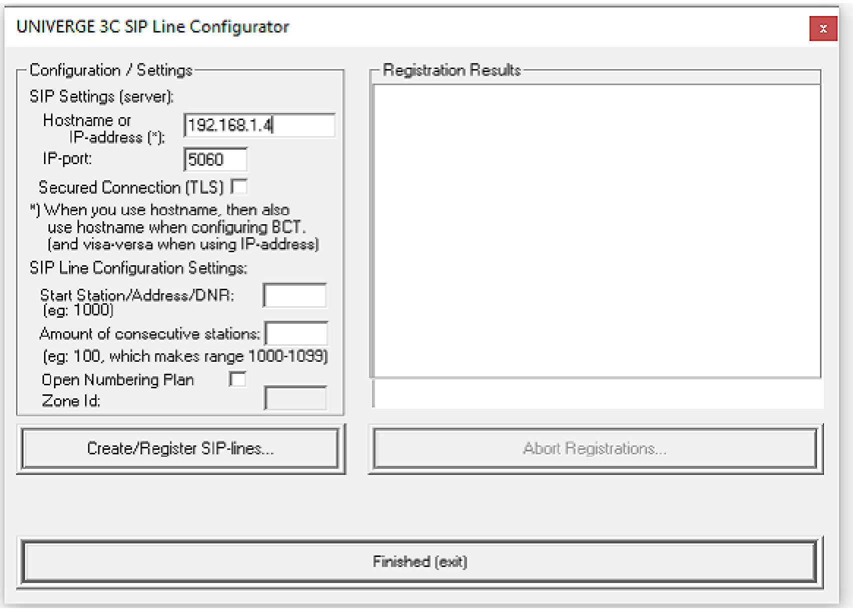
4.6.3. UNIVERGE 3C SIP Line Configurator

The “UNIVERGE 3C SIP Line Configurator” is a tool which creates SIP Stations in UNIVERGE 3C for use by BCT. It can be found on the Business ConneCT installation DVD, which should automatically start when you place it in your DVD drive. Select “Configuration Support” under the section “Additional Resources” and run the “SIPLineConfigurator.exe” from the sub-folder “SIP Line Configurator”.

Note: *If DVD does not automatically start it can be started manually via Start → Run and entering <DVD Drive>:\autorun.exe*

Note: *You must have local administrator rights to run the “UNIVERGE 3C SIP Line Configurator”.*

Note: *The UNIVERGE 3C SIP Line Configurator can be found in folder” D:\Business ConneCT Resources\Configuration Support\SIP Line Configurator” (where D is the line drive letter of your DVD drive).*



UNIVERGE 3C SIP Line Configurator

Configuration / Settings

SIP Settings (server):

Hostname or IP-address (*): 192.168.1.4

IP-port: 5060

Secured Connection (TLS) □

*) When you use hostname, then also use hostname when configuring BCT. (and visa-versa when using IP-address)

SIP Line Configuration Settings:

Start Station/Address/DNR: (eg: 1000)

Amount of consecutive stations: (eg: 100, which makes range 1000-1099)

Open Numbering Plan □

Zone Id:

Registration Results

1. UNIVERGE 3C SIP Settings:

IP-address: Enter the Hostname or IP address of the UNIVERGE 3C Server
Note: when "Hostname" is used, then also use "Hostname" for configuring BCT. Otherwise use IP-address in both cases.

IP-port: Enter the IP port used by SIP (default is 5060)

2. SIP Line Configuration Settings:

Start Station/Address/DNR: Enter the first station (address / DNR) number in the range which is to be assigned.

Amount of consequent stations: Enter the total number of stations to be created

Open Numbering Plan: Check when UNIVERGE 3C server has Open Numbering Plan enabled

Zone Id: Enter the Zone Id (integer value) CtiUser has zone rights on. (Only for Open Numbering Plan)

3. Click the **Create/Register SIP-lines...** button.

The **Registration Results** window should display a message similar to this example which shows Station 4954 being created on a UNIVERGE 3C Server located at 192.168.1.4;

```
START Registration... (check/wait for OK/FAIL’s)
Register   : “4954”<sip:4954@192.168.1.4:5060>
END Sent Registrations...(wait for OK/FAIL’s(max 32 sec))
Register Rsp: OK >4954
```

4. Repeat steps 2 & 3 until all required stations have been created.

5. Click the **Finished (exit)** button to close the UNIVERGE 3C SIP Line Configurator.

4.6.3.1. Example Assignment (Open Numbering Plan not enabled)

The chart below shows all of the Stations & Extensions which will be assigned in UNIVERGE 3C for use with BCT. Note that only the highlighted numbers in this example must be assigned with the UNIVERGE 3C SIP Line Configurator. Numbers which are not highlighted are created manually in UNIVERGE 3C. So for e.g. the VMP lines, start station would 4900 with consequent amount 4.

	UNIVERGE 3C		
	Extension	Station	Used For
Operator	9	9	Internal Access
	4950	4950	External Access
	4951	4951	Park
	4960	4960	Pickup Park (also called System Call Park)
	4961		Pickup Park pos. 1
	4962 etc.		Pickup Park pos. 2 etc.
	4952	4952	Fallback

	UNIVERGE 3C		
	Extension	Station	Used For
Call Center	4040	4954	Call Center Pilot
	4043		Agent Logon
	4044		Prompt Recording
	4954		Messagebox

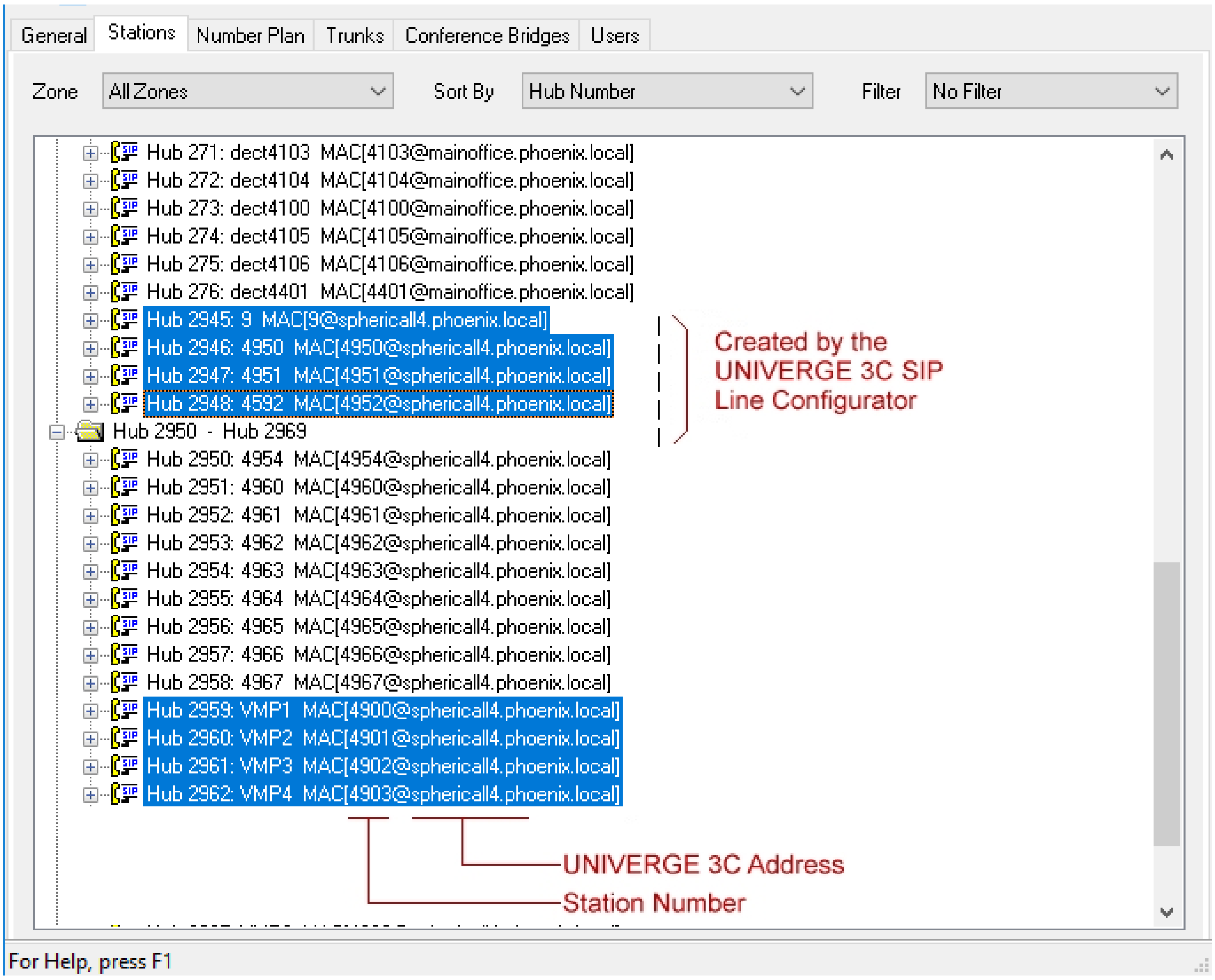
	UNIVERGE 3C		
VMP	Extension	Station	Used For

	4900	4900	VMP Line
	4901	4901	VMP Line
	4902	4902	VMP Line
	4903	4903	VMP Line
	4953	4900 4901 4902 4903	Round Robin Group

	First Assignment	Second Assignment	Third Assignment	Fourth Assignment
Start DNR:	9	4950	4900	4953
Amount of DNR's:	1	3	4	1

Note: *VMP Lines, Operator Numbers (internal, external, failover, park, system call park), and Contact Center Numbers (pilots, agent logon, messagebox access, prompt recording) will all register at the same UNIVERGE 3C UCM server as BCT is connected to. They cannot be distributed over a multi UNIVERGE 3C server system.*

Once the stations have been created, they should appear in the UNIVERGE 3C Administrator as shown below:



Zone: All Zones
Sort By: Hub Number
Filter: No Filter

```
Hub 271: dect4103  MAC[4103@mainoffice.phoenix.local]
Hub 272: dect4104  MAC[4104@mainoffice.phoenix.local]
Hub 273: dect4100  MAC[4100@mainoffice.phoenix.local]
Hub 274: dect4105  MAC[4105@mainoffice.phoenix.local]
Hub 275: dect4106  MAC[4106@mainoffice.phoenix.local]
Hub 276: dect4401  MAC[4401@mainoffice.phoenix.local]
Hub 2945: 9  MAC[9@sphericall4.phoenix.local]
Hub 2946: 4950  MAC[4950@sphericall4.phoenix.local]
Hub 2947: 4951  MAC[4951@sphericall4.phoenix.local]
Hub 2948: 4592  MAC[4952@sphericall4.phoenix.local]
Hub 2950 - Hub 2969
Hub 2950: 4954  MAC[4954@sphericall4.phoenix.local]
Hub 2951: 4960  MAC[4960@sphericall4.phoenix.local]
Hub 2952: 4961  MAC[4961@sphericall4.phoenix.local]
Hub 2953: 4962  MAC[4962@sphericall4.phoenix.local]
Hub 2954: 4963  MAC[4963@sphericall4.phoenix.local]
Hub 2955: 4964  MAC[4964@sphericall4.phoenix.local]
Hub 2956: 4965  MAC[4965@sphericall4.phoenix.local]
Hub 2957: 4966  MAC[4966@sphericall4.phoenix.local]
Hub 2958: 4967  MAC[4967@sphericall4.phoenix.local]
Hub 2959: VMP1  MAC[4900@sphericall4.phoenix.local]
Hub 2960: VMP2  MAC[4901@sphericall4.phoenix.local]
Hub 2961: VMP3  MAC[4902@sphericall4.phoenix.local]
Hub 2962: VMP4  MAC[4903@sphericall4.phoenix.local]
```

Created by the UNIVERGE 3C SIP Line Configurator

UNIVERGE 3C Address

Station Number

For Help, press F1

4.6.3.2. Example Assignment (Open Numbering Plan enabled)

Suppose CtiUser has zone rights in zone “Company-A” with zone id integer value 7 (see [8.1.5 Connection to PBX]() “Zone selection” how to retrieve the value of the zone id).
In the UNIVERGE 3C SIP Line Configurator, check the checkbox “Open Numbering Plan” and enter value 7 in “Zone Id”.
All stations created with the UNIVERGE 3C SIP Line Configurator will get a suffix to discriminate between zones. The suffix added is in form of “-(<zoneId>)”.
So in this example e.g. the stations created for the VMP lines will be 4900-(7) until 4903-(7) etc.

The chart below shows all of the Stations & Extensions which will be assigned in UNIVERGE 3C for use with BCT. Note that only the highlighted numbers in this example must be assigned with the UNIVERGE 3C SIP Line Configurator. Numbers which are not highlighted are created manually in UNIVERGE 3C. So for e.g. the VMP lines, start station would 4900 with consequent amount 4.

	UNIVERGE 3C		
	Extension	Station	Used For
Operator	9	9	Internal Access
	4950	4950	External Access
	4951	4951	Park
	4960	4960	Pickup Park (also called System Call Park)
	4961		Pickup Park pos. 1
	4962 etc.		Pickup Park pos. 2 etc.
	4952	4952	Fallback

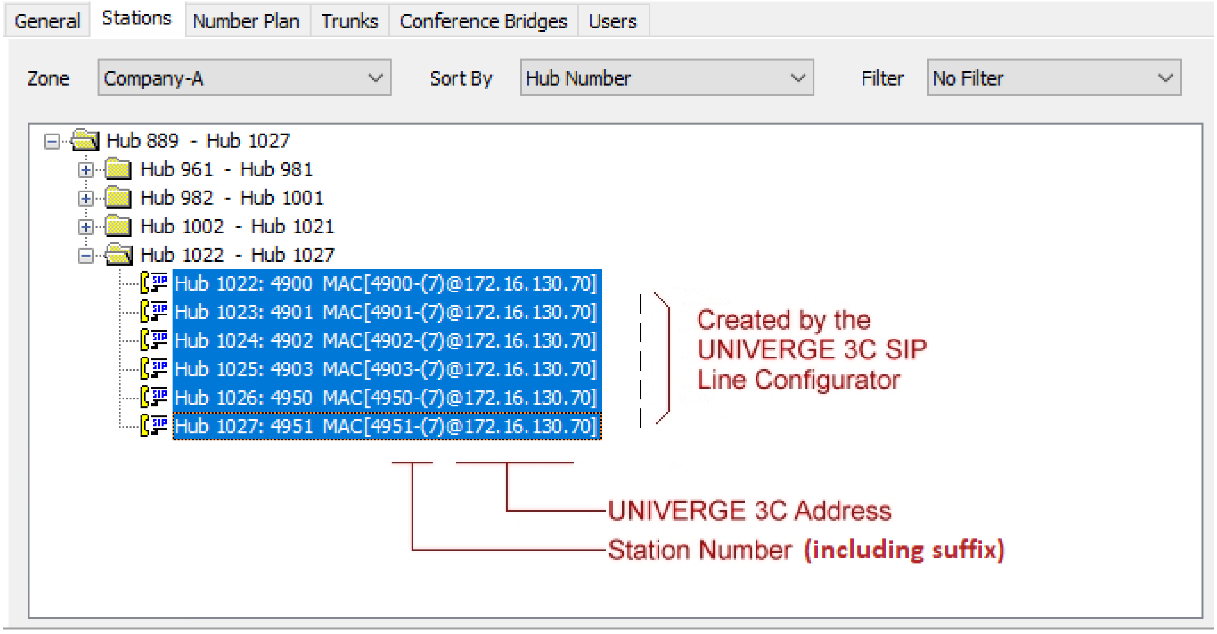
	UNIVERGE 3C		
	Extension	Station	Used For
Call Center	4040	4954	Call Center Pilot
	4043		Agent Logon
	4044		Prompt Recording
	4954		Messagebox

	UNIVERGE 3C		
	Extension	Station	Used For
VMP Lines	4900	4900	VMP Line
	4901	4901	VMP Line
	4902	4902	VMP Line
	4903	4903	VMP Line
	4953	4900 4901 4902 4903	Round Robin Group

	First Assignment	Second Assignment	Third Assignment	Fourth Assignment
Start DNR:	9	4950	4900	4953
Amount of DNR’s:	1	3	4	1
Open Numbering Plan:	**Checked**	**Checked**	**Checked**	**Checked**
Zone Id:	**7**	**7**	**7**	**7**

Note: *VMP Lines, Operator Numbers (internal, external, failover, park, system call park), and Contact Center Numbers (pilots, agent logon, messagebox access, prompt recording) will all register at the same UNIVERGE 3C UCM server as BCT is connected to. They cannot be distributed over a multi UNIVERGE 3C server system.*

Once the stations have been created, they will appear in the UNIVERGE 3C Administrator.
To be able to use the stations within the zone “Company-A”, modify the zone within the station properties and select “Company-A” and they will as shown below:



Zone: Company-A
Sort By: Hub Number
Filter: No Filter

```
Hub 889 - Hub 1027
    Hub 961 - Hub 981
    Hub 982 - Hub 1001
    Hub 1002 - Hub 1021
    Hub 1022 - Hub 1027
        Hub 1022: 4900  MAC[4900-(7)@172.16.130.70]
        Hub 1023: 4901  MAC[4901-(7)@172.16.130.70]
        Hub 1024: 4902  MAC[4902-(7)@172.16.130.70]
        Hub 1025: 4903  MAC[4903-(7)@172.16.130.70]
        Hub 1026: 4950  MAC[4950-(7)@172.16.130.70]
        Hub 1027: 4951  MAC[4951-(7)@172.16.130.70]
```

Created by the UNIVERGE 3C SIP Line Configurator

UNIVERGE 3C Address

Station Number **(including suffix)**

4.6.4. UNIVERGE 3C configuration

4.6.4.1. Preconditions

Log into the UNIVERGE 3C Server with the “SRV3Csupport” (or “SphereSupport” on older systems) account (or equivalent account which has administrator rights).

4.6.4.2. Edit UNIVERGE 3C System Properties

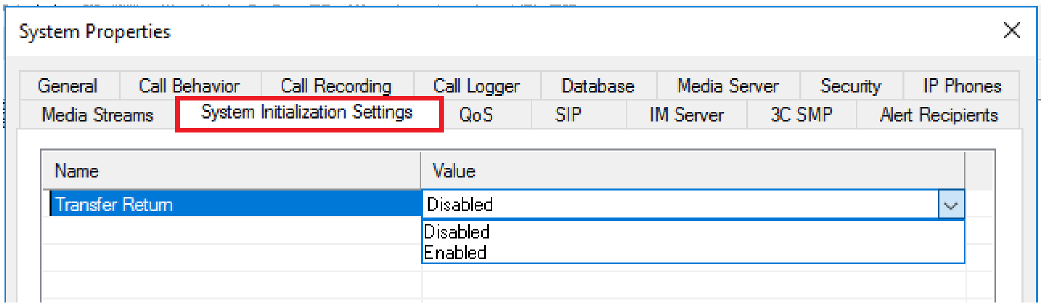
There are three items to set in System Properties; set the Transfer Return timer, disable Transfer Return (system), and configure out of band DTMF.

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. In the General tab, double click the organization name to access the **System properties** window.

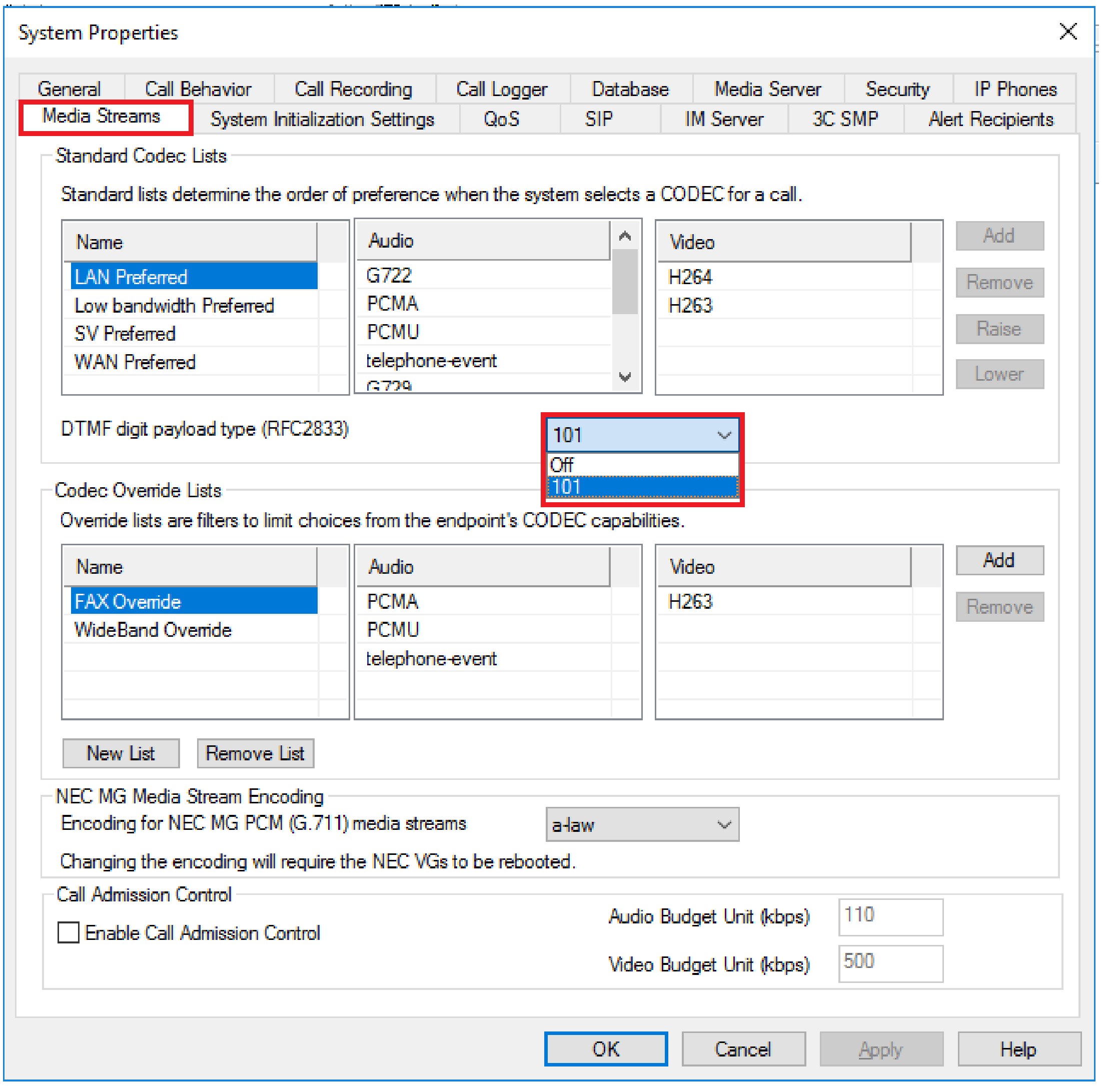
3. Go to the "System Initialization Settings" tab and click the **Add** button.

4. Double click the selected line and scroll down the list for “Transfer Return” and set it to disabled. See the following figure.



Name	Value
Transfer Return	Disabled

5. Go to the tab "Media Streams". Set the "DTMF digit payload type (RFC2833)" to 101, and then click **OK**. See the following figure.



Standard Codec Lists

Standard lists determine the order of preference when the system selects a CODEC for a call.

Name	Audio	Video
LAN Preferred	G722	H264
Low bandwidth Preferred	PCMA	H263
SV Preferred	PCMU	
WAN Preferred	telephone-event	
	G729	

DTMF digit payload type (RFC2833): 101

Codec Override Lists

Override lists are filters to limit choices from the endpoint's CODEC capabilities.

Name	Audio	Video
FAX Override	PCMA	H263
WideBand Override	PCMU	
	telephone-event	

NEC MG Media Stream Encoding

Encoding for NEC MG PCM (G.711) media streams: a-law

Changing the encoding will require the NEC VGs to be rebooted.

Call Admission Control

□ Enable Call Admission Control

Audio Budget Unit (kbps): 110

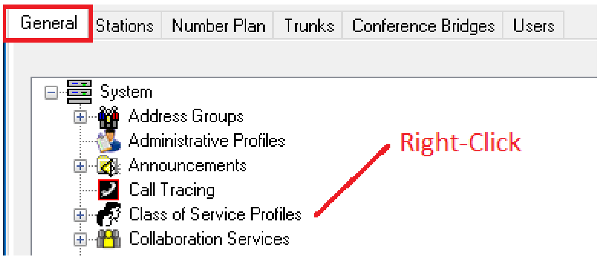
Video Budget Unit (kbps): 500

4.6.4.3. Class of Service

Create three new Classes of Service for use with BCT Agent/Operator users, Routing Points and VMP lines.

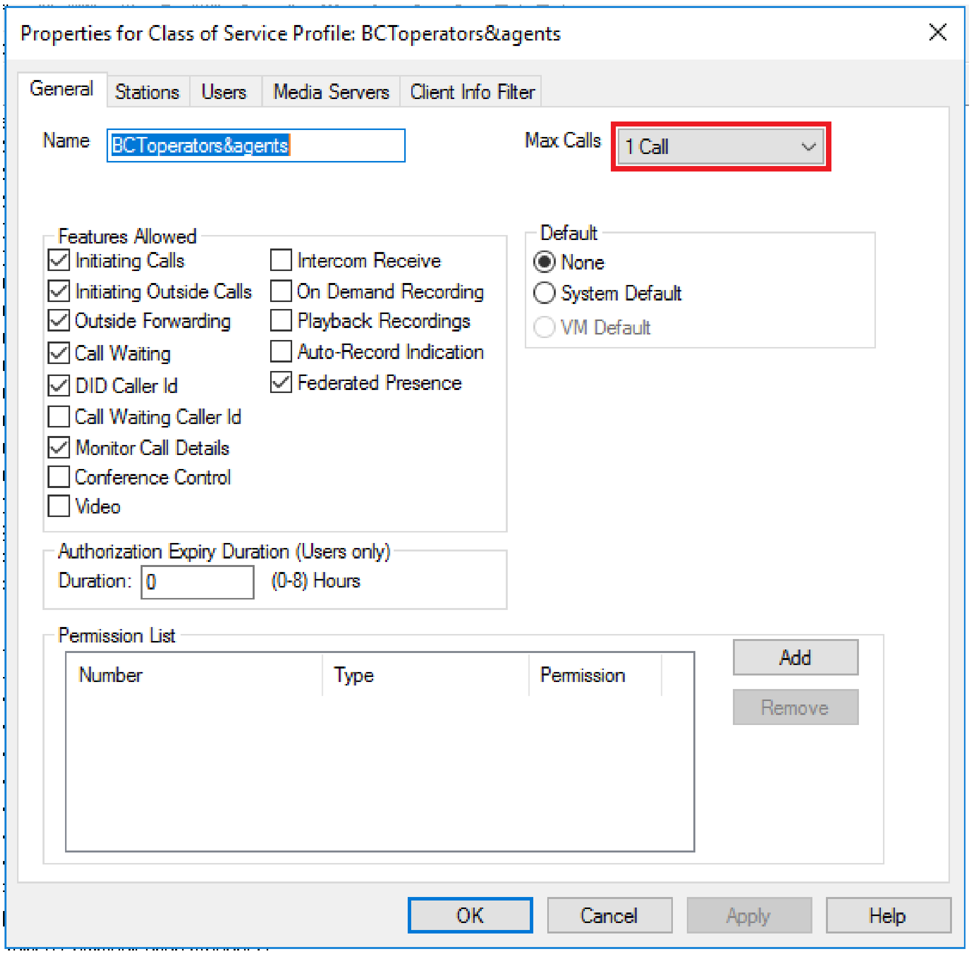
1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. In the General tab, expand the Organization Name, right click Class of Service Profiles and select **Add**. The Properties for **New Class of Service Profile** window will open.



3. Enter the following information then click **OK**.

Name:	BCT operators&agents
Max Calls:	1 Call



Properties for Class of Service Profile: BCToperators&agents

Name: BCToperators&agents

Max Calls: 1 Call

Features Allowed
- ☑ Initiating Calls
- ☑ Initiating Outside Calls
- ☑ Outside Forwarding
- ☑ Call Waiting
- ☑ DID Caller Id
- □ Call Waiting Caller Id
- ☑ Monitor Call Details
- □ Conference Control
- □ Video
- □ Intercom Receive
- □ On Demand Recording
- □ Playback Recordings
- □ Auto-Record Indication
- ☑ Federated Presence

Default
- ● None
- ○ System Default
- ○ VM Default

Authorization Expiry Duration (Users only)

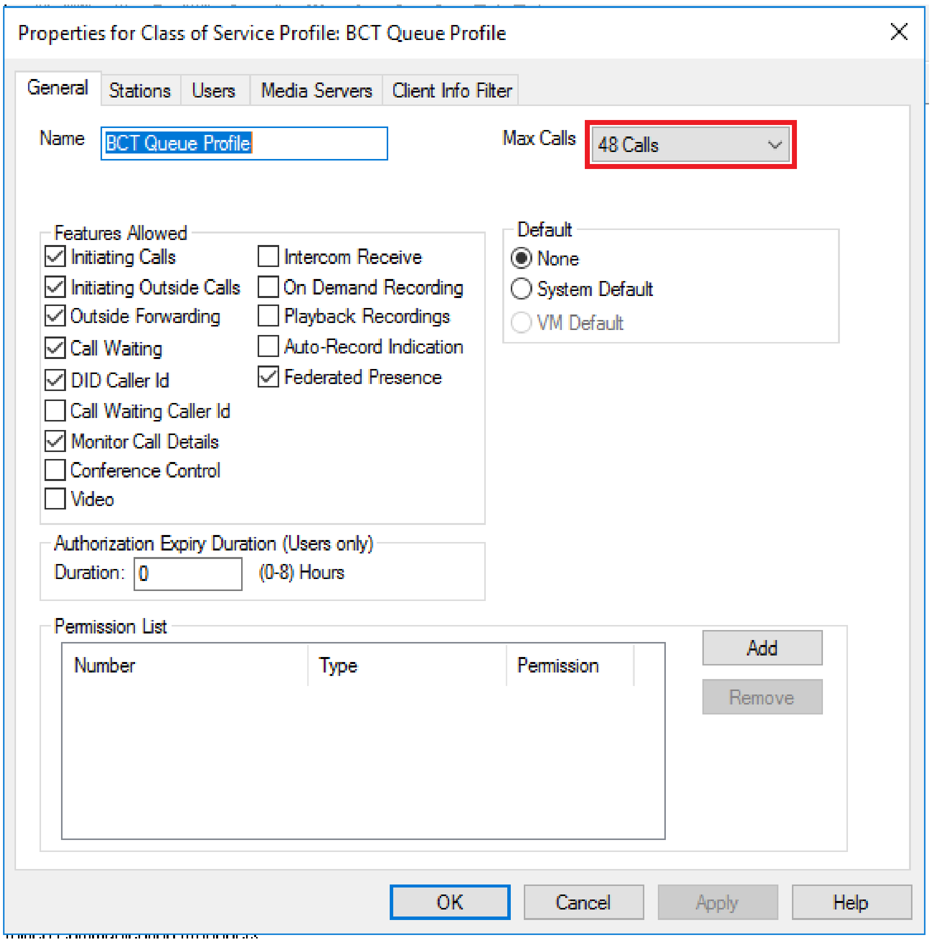
Duration: 0 (0-8) Hours

Permission List

Number	Type	Permission

1. Add a second new Class of Service with the following information and then click **OK**.

   Name: BCT Queue Profile
   Max Calls: 48 Calls



Properties for Class of Service Profile: BCT Queue Profile

Name: BCT Queue Profile

Max Calls: 48 Calls

Features Allowed
☑ Initiating Calls
☑ Initiating Outside Calls
☑ Outside Forwarding
☑ Call Waiting
☑ DID Caller Id
□ Call Waiting Caller Id
☑ Monitor Call Details
□ Conference Control
□ Video
□ Intercom Receive
□ On Demand Recording
□ Playback Recordings
□ Auto-Record Indication
☑ Federated Presence

Default
● None
○ System Default
○ VM Default

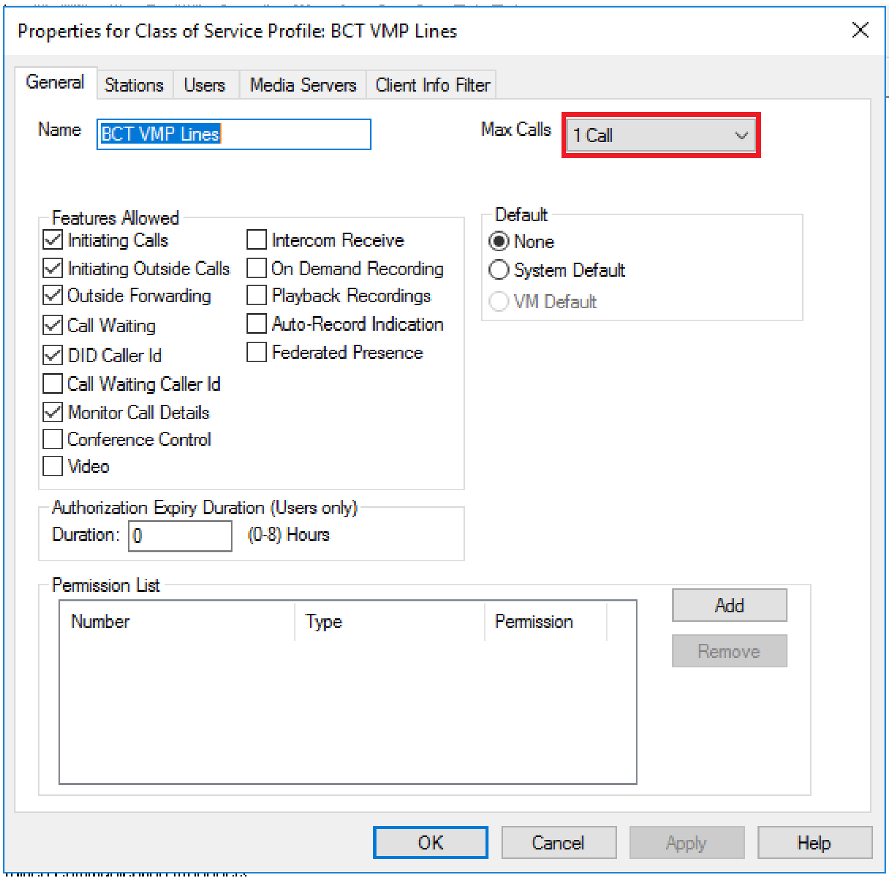
Authorization Expiry Duration (Users only)
Duration: 0 (0-8) Hours

Permission List

Number	Type	Permission

2. Add a third new Class of Service with the following information and then click **OK**.

Name: BCT VMP Lines
Max Calls: 1 Call



Name: BCT VMP Lines
Max Calls: 1 Call

Features Allowed
☑ Initiating Calls
☑ Initiating Outside Calls
☑ Outside Forwarding
☑ Call Waiting
☑ DID Caller Id
□ Call Waiting Caller Id
☑ Monitor Call Details
□ Conference Control
□ Video
□ Intercom Receive
□ On Demand Recording
□ Playback Recordings
□ Auto-Record Indication
□ Federated Presence

Default
● None
○ System Default
○ VM Default

Authorization Expiry Duration (Users only)
Duration: 0 (0-8) Hours

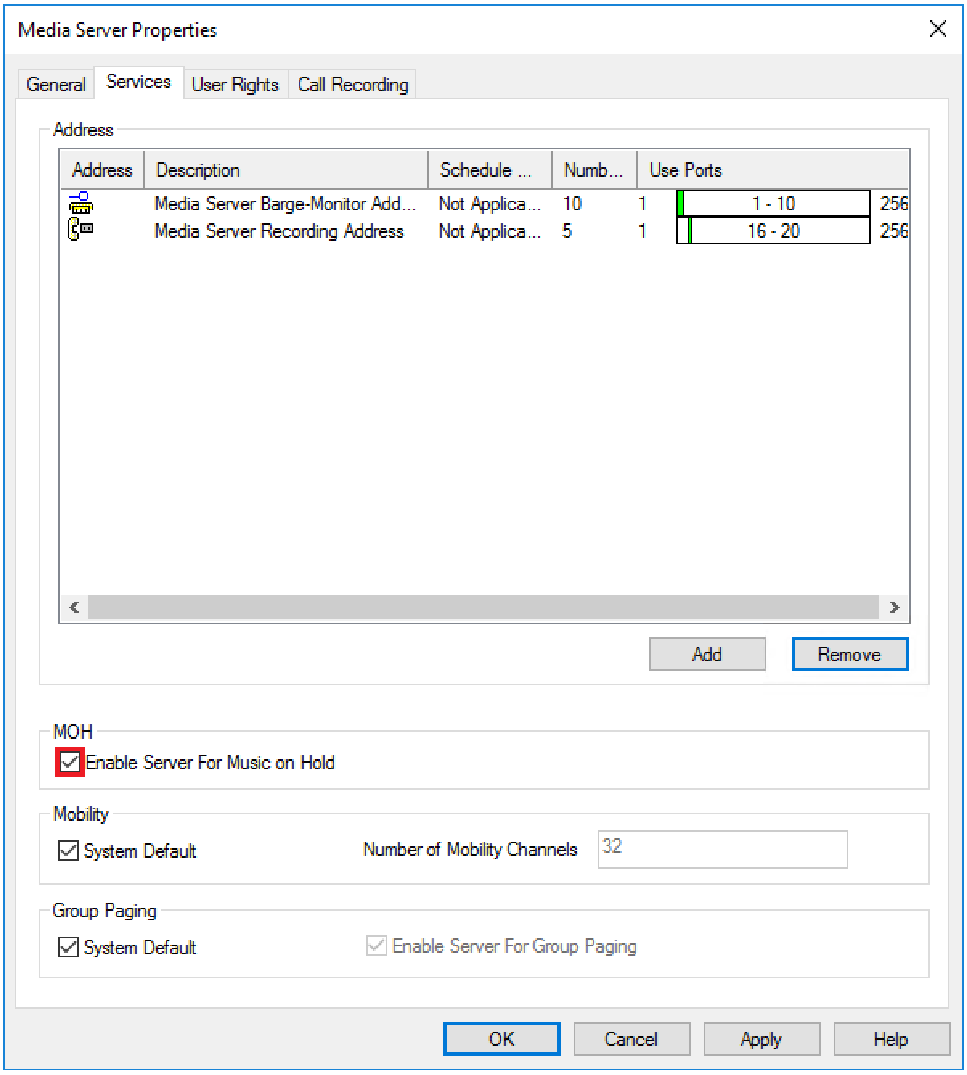
4.6.4.4. Music On Hold

- UNIVERGE 3C MOH is given when a call is put on hold by a user, and another outgoing call is made (consultation).
- No MOH (but ring-tone) is given when a call is located on a routing point or a call is routed from a routing point to an agent.
- BCT MOH is provided while a call is in the BCT router-queue and router-configuration indicates that MOH is to be provided. BCT MOH is given from a VMP line.
- When configured, calls can be routed to an agent from a VMP line, see 8.4.3 How to disable "Route Calls From Routing Point”. In this case UNIVERGE 3C MOH will be applied (possibly after BCT MOH has been provided).

In case you want to switch off UNIVERGE 3C MOH, follow these steps:

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. In the general tab, expand the organization name and Media Servers, double click the media server name. In the Media server properties window, check mark "Enable Server For Music On Hold" in the UNIVERGE 3C MOH box and click **OK**. See the following figure:



Address

Address	Description	Schedule ...	Numb...	Use Ports		
	Media Server Barge-Monitor Add...	Not Applica...	10	1	1 - 10	256
	Media Server Recording Address	Not Applica...	5	1	16 - 20	256

MOH

☑ Enable Server For Music on Hold

Mobility

☑ System Default

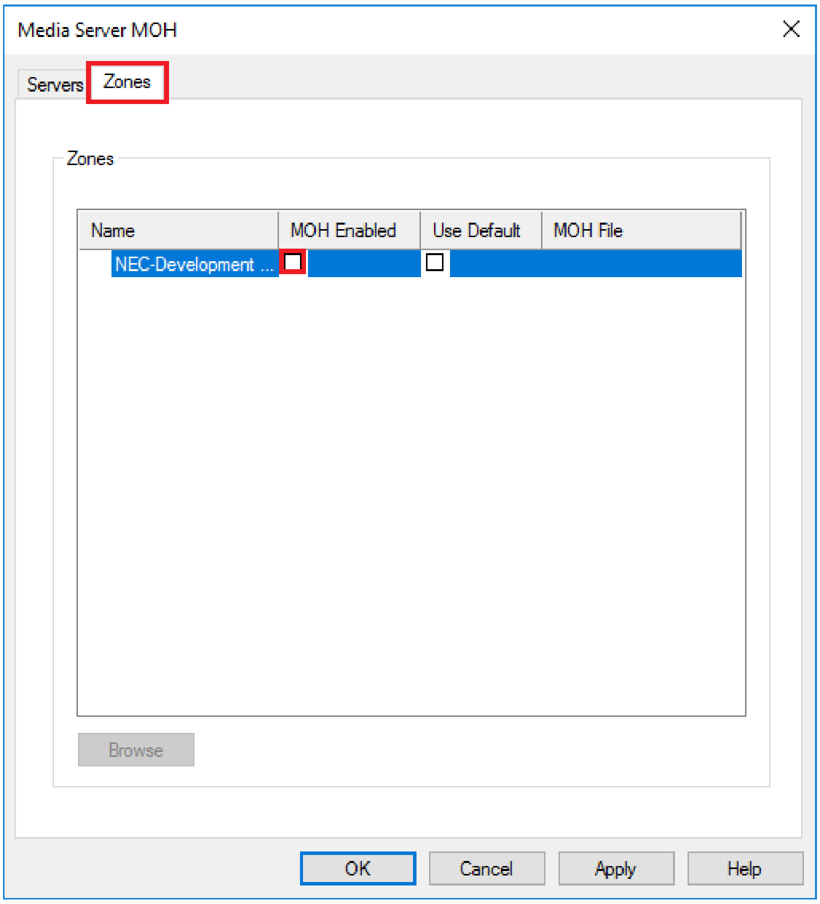
Number of Mobility Channels 32

Group Paging

☑ System Default

☑ Enable Server For Group Paging

3. In the general tab, expand the organization name and expand Music on Hold and double click the Media Server MOH, now go to tab Zones and make sure the MOH Enabled box is unchecked. Click **OK** to confirm.



Name	MOH Enabled	Use Default	MOH File
NEC-Development ...	□	□	

4.6.4.5. Configure Operator Stations

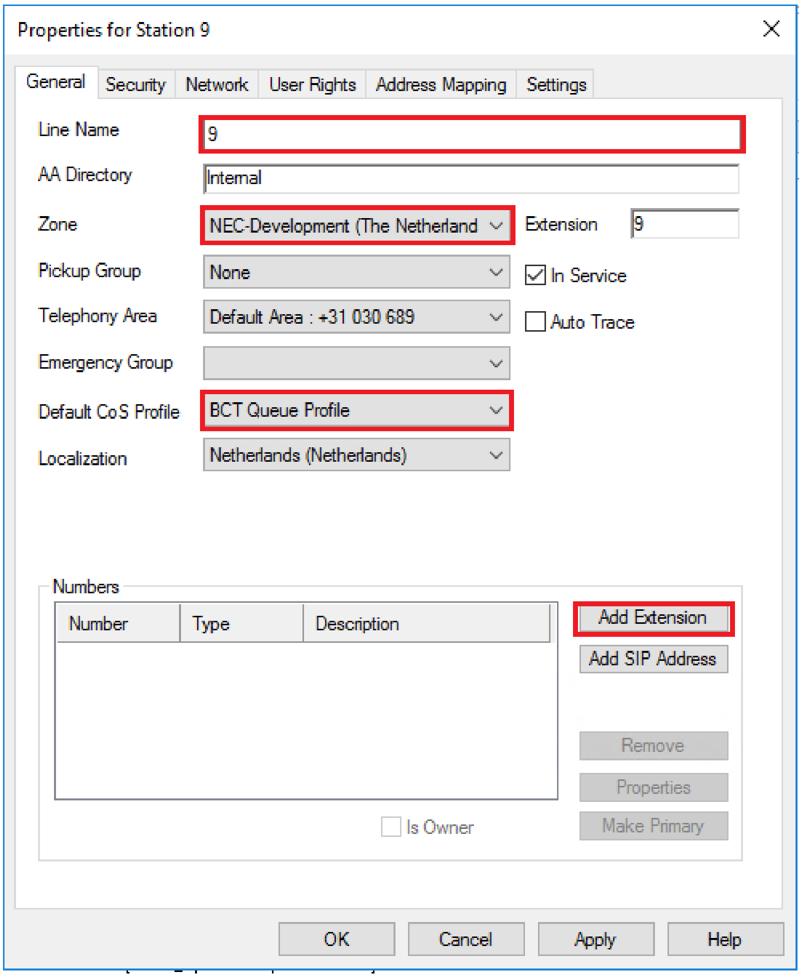
In our example there are seven numbers associated with the BCT Operator (see 4.6.1.4 Operator configuration);

Number used by Internal Parties:	9
Number used by External Parties:	4950
Number used to Park calls:	4951
Number used by System Call Park: (also called Pickup Park)	4960 ~ 4962
Number used by Failed calls:	4952

Note: *Numbers associated with the Operator cannot register on multi UNIVERGE 3C UCM servers, they must register at the same UNIVERGE 3C UCM server as BCT is connected to.*

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. Go to the “Stations” tab and look for the 4 hub numbers which were added by the UNIVERGE 3C SIP Line Configurator (*see the example in Part Three*). Double-Click on the HUB for station “9”.



Properties for Station 9

Line Name: 9

AA Directory: Internal

Zone: NEC-Development (The Netherland

Extension: 9

Pickup Group: None

☑ In Service

Telephony Area: Default Area : +31 030 689

☐ Auto Trace

Emergency Group:

Default CoS Profile: BCT Queue Profile

Localization: Netherlands (Netherlands)

Numbers

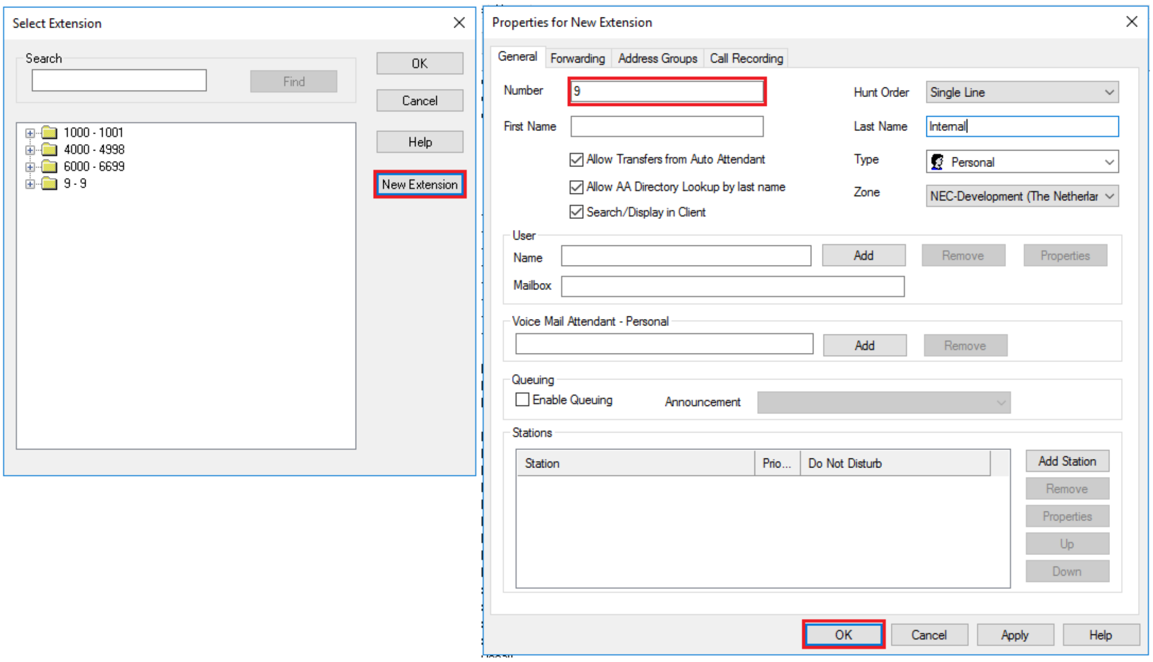
Number	Type	Description

☐ Is Owner

3. In the **Properties for Station** window, choose the General tab and enter the following;

Line Name: Optional – Enter a descriptive name such as “9”
Zone: Choose the zone from the pull-down menu
Pickup Group: Leave default “None”
Telephony Area: Leave default or choose a new one from the pull-down menu
Emergency Group: Leave blank
Default CoS Profile: Choose “BCT Queue Profile” from the pull-down menu (see 4.6.4.3 Class of Service)
Localization: Select your location or leave default “Netherlands (Netherlands)”

4. Now you must assign extension numbers to stations. To assign extensions first click **Add extension** and in the **Select Extension** window click **New Extension**. Now the **Properties for new extension** window opens.


Select Extension

Search

1000 - 1001
4000 - 4998
6000 - 6699
9 - 9

Properties for New Extension

General | Forwarding | Address Groups | Call Recording

Number: 9

First Name:

Hunt Order: Single Line

Last Name: Internal

Type: Personal

Zone: NEC-Development (The Netherlar

☑ Allow Transfers from Auto Attendant

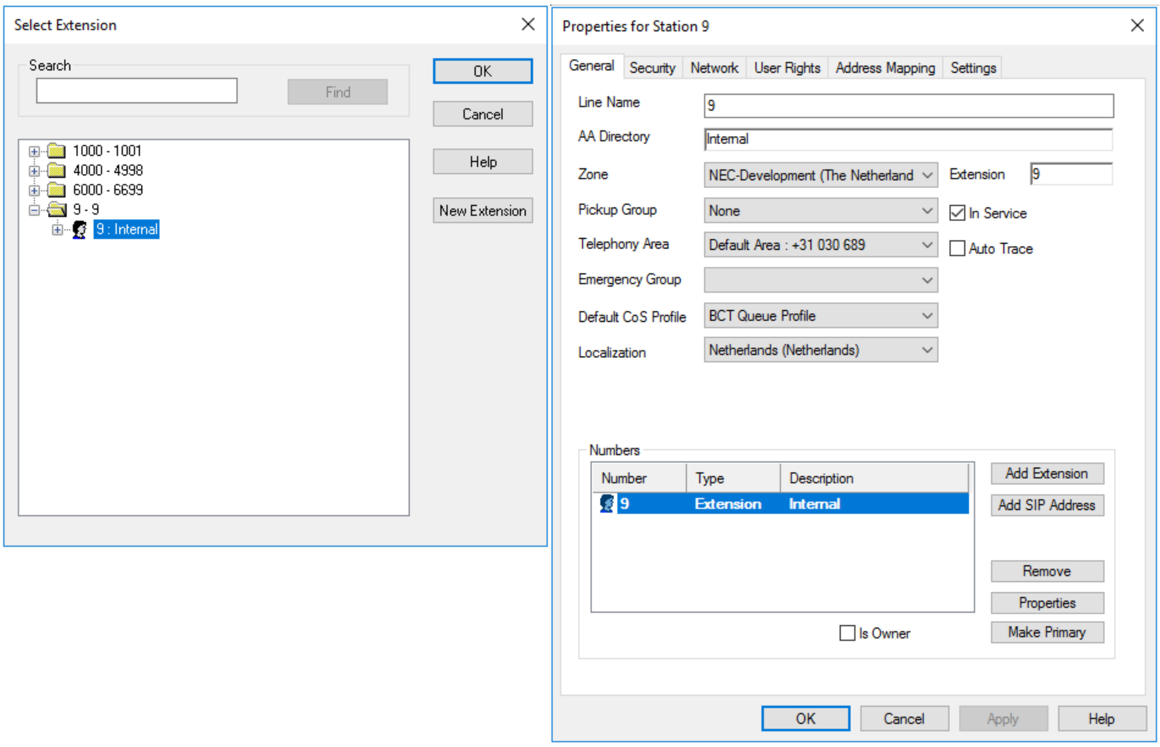
☑ Allow AA Directory Lookup by last name

☑ Search/Display in Client

Queuing: □ Enable Queuing

5. Enter extension number “9” in the Number field. The First and Last Name fields are optional. Then click **OK**.

6. You then return to the "Select Extension" window. Select extension “9” from the list and click **OK** twice.


Select Extension

1000 - 1001
4000 - 4998
6000 - 6699
9 - 9
9 : Internal

Properties for Station 9

General | Security | Network | User Rights | Address Mapping | Settings

Line Name: 9

AA Directory: Internal

Zone: NEC-Development (The Netherland

Extension: 9

Pickup Group: None

☑ In Service

Telephony Area: Default Area : +31 030 689

□ Auto Trace

Emergency Group:

Default CoS Profile: BCT Queue Profile

Localization: Netherlands (Netherlands)

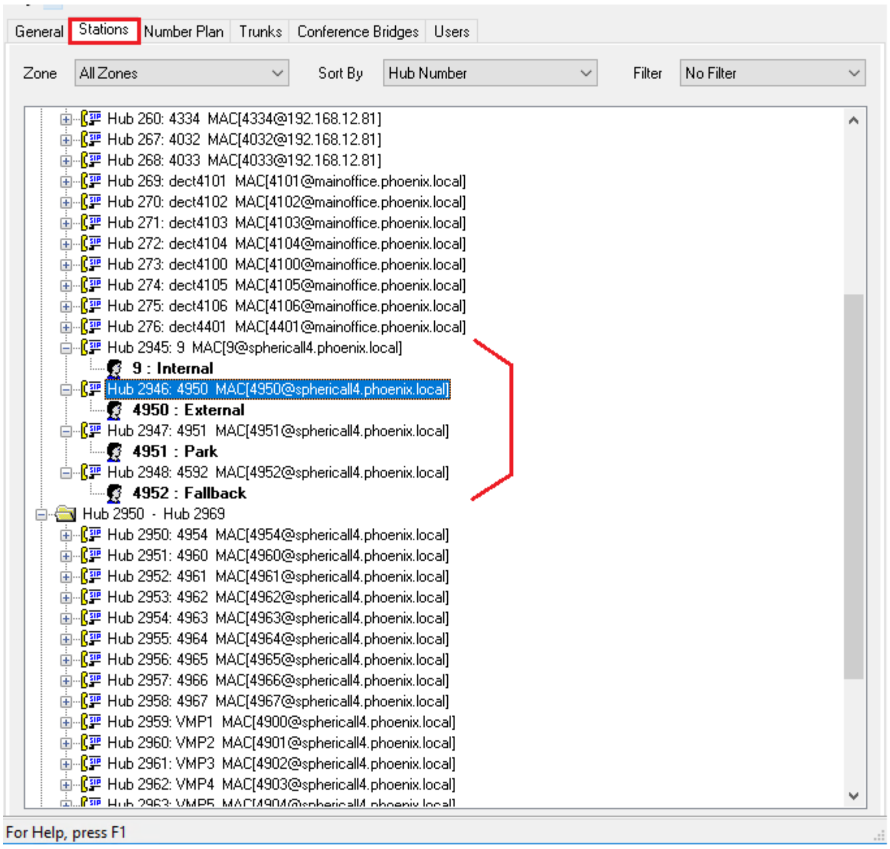
Number	Type	Description
9	Extension	Internal

□ Is Owner

7. Repeat steps 2 – 6 for stations 4950, 4951, 4952 and 4960 ~ 4962.

Note: *For System Call Park (also called Pickup Park) the first number (4960) is used as station, and the related extension range (4961 ~ 4962) are used as positions to park individual calls. All used stations (4960, 4961 and 4962) should be stations with extensions assigned to them. For BCT configuration for System Call Park see* [8.3.10 Create System Call Park configuration](#).

8. In the “Stations” tab you can see that extensions have been added to the stations, as shown in the next figure:



Zone: All Zones Sort By: Hub Number Filter: No Filter

```
  Hub 260: 4334  MAC[4334@192.168.12.81]
  Hub 267: 4032  MAC[4032@192.168.12.81]
  Hub 268: 4033  MAC[4033@192.168.12.81]
  Hub 269: dect4101  MAC[4101@mainoffice.phoenix.local]
  Hub 270: dect4102  MAC[4102@mainoffice.phoenix.local]
  Hub 271: dect4103  MAC[4103@mainoffice.phoenix.local]
  Hub 272: dect4104  MAC[4104@mainoffice.phoenix.local]
  Hub 273: dect4100  MAC[4100@mainoffice.phoenix.local]
  Hub 274: dect4105  MAC[4105@mainoffice.phoenix.local]
  Hub 275: dect4106  MAC[4106@mainoffice.phoenix.local]
  Hub 276: dect4401  MAC[4401@mainoffice.phoenix.local]
  Hub 2945: 9  MAC[9@sphericall4.phoenix.local]
      9 : Internal
  Hub 2946: 4950  MAC[4950@sphericall4.phoenix.local]
      4950 : External
  Hub 2947: 4951  MAC[4951@sphericall4.phoenix.local]
      4951 : Park
  Hub 2948: 4592  MAC[4952@sphericall4.phoenix.local]
      4952 : Fallback
Hub 2950 - Hub 2969
  Hub 2950: 4954  MAC[4954@sphericall4.phoenix.local]
  Hub 2951: 4960  MAC[4960@sphericall4.phoenix.local]
  Hub 2952: 4961  MAC[4961@sphericall4.phoenix.local]
  Hub 2953: 4962  MAC[4962@sphericall4.phoenix.local]
  Hub 2954: 4963  MAC[4963@sphericall4.phoenix.local]
  Hub 2955: 4964  MAC[4964@sphericall4.phoenix.local]
  Hub 2956: 4965  MAC[4965@sphericall4.phoenix.local]
  Hub 2957: 4966  MAC[4966@sphericall4.phoenix.local]
  Hub 2958: 4967  MAC[4967@sphericall4.phoenix.local]
  Hub 2959: VMP1  MAC[4900@sphericall4.phoenix.local]
  Hub 2960: VMP2  MAC[4901@sphericall4.phoenix.local]
  Hub 2961: VMP3  MAC[4902@sphericall4.phoenix.local]
  Hub 2962: VMP4  MAC[4903@sphericall4.phoenix.local]
  Hub 2963: VMP5  MAC[4904@sphericall4.phoenix.local]
```

For Help, press F1

9. To configure operators being able to hande external calls that encounter a busy, not answering , do not disturb or non-existing condition see *Appendix N-1 – Configure Operator Fallback for failed external calls*

10. To configure operators being able to break-in into a conversation see *Appendix N-4 – Operator Break-In*

11. By using the Class of service “BCT Queue Profile” a maximum of 48 calls can be queued on a single routing point. If more calls need to be queued on a routing point then you need to add the Line setting “Station Max Calls Override”. To do this open the properties of the station of the routing point, go to tab Settings, press button Add, select the setting “Station Max Call Override” from the dropdown list and give it the required value. The maximum value BCT can handle is 200.

4.6.4.6. Configure VMP Lines

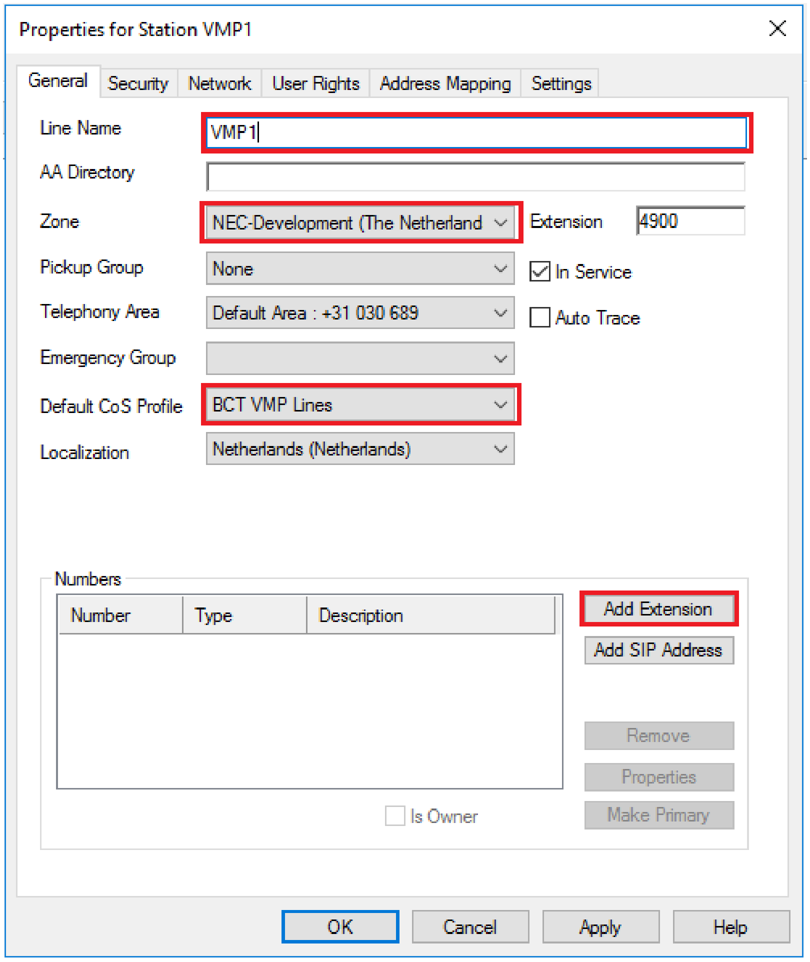
Before you start, you have to define how many VMP lines you need to configure in your system.

In the following example 4 VMP lines are configured. This means that only 4 callers at a time can hear voice prompts (e.g. queue prompts or messagebox prompts) or hear music on hold simultaneously. Should the system encounter a situation that all 4 VMP lines are occupied, then no prompt or music on hold is played (silence). You can decide to either increase or decrease the number of VMP lines as presented in this example.

Note: *VMP lines cannot be distributed over a multi UNIVERGE 3C server system, they must reside in the primary UNIVERGE 3C server.*

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. Go to the "Stations" tab and look for the 4 hub numbers which were added by the UNIVERGE 3C SIP Line Configurator (*see the example in Part Three*). Double-Click on the HUB for station "4900".



Properties for Station VMP1

Line Name: VMP1
AA Directory:
Zone: NEC-Development (The Netherland
Extension: 4900
Pickup Group: None
☑ In Service
Telephony Area: Default Area : +31 030 689
□ Auto Trace
Emergency Group:
Default CoS Profile: BCT VMP Lines
Localization: Netherlands (Netherlands)

Numbers

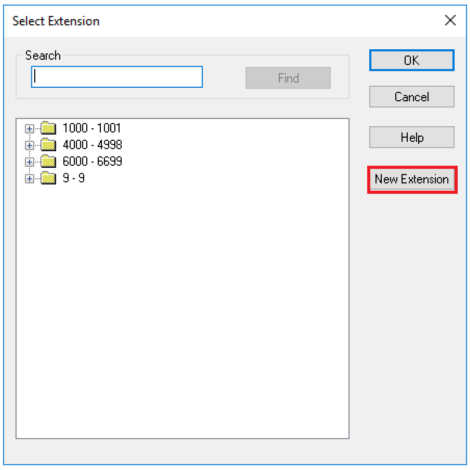
Number	Type	Description

□ Is Owner

3. In the **Properties for Station** window, choose the General tab and enter the following;

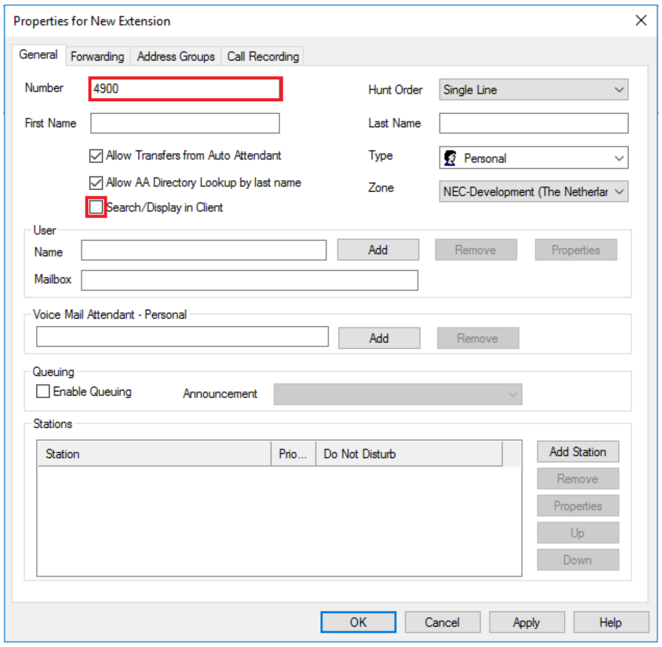
Line Name:	Optional – Enter a descriptive name such as "VMP1"
Zone:	Choose the zone from the pull-down menu
Pickup Group:	Leave default "None"
Telephony Area:	Leave default or choose a new one from the pull-down menu
Emergency Group:	Leave blank
Default CoS Profile:	Choose "BCT VMP Lines" from the pull-down menu
Localization:	Select your location or leave default "Netherlands (Netherlands)"

4. Now you must assign extension numbers to stations. To assign extensions first click **Add extension** and in the **Select Extension** window click **New Extension**. Now the **Properties for new extension** window opens.


Select Extension

Search:

1000 - 1001
4000 - 4998
6000 - 6699
9 - 9


Properties for New Extension

General | Forwarding | Address Groups | Call Recording

Number: 4900
First Name:
Hunt Order: Single Line
Last Name:
Type: Personal
Zone: NEC-Development (The Netherlar

☑ Allow Transfers from Auto Attendant
☑ Allow AA Directory Lookup by last name
□ Search/Display in Client

User
Name:
Mailbox:

Voice Mail Attendant - Personal

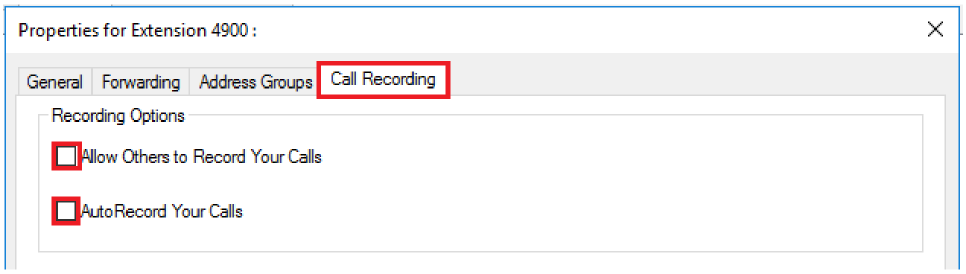
Queuing
□ Enable Queuing
Announcement:

Stations

Station	Prio...	Do Not Disturb

5. Enter extension number “4900” in the Number field. Uncheck “Search/Display in Client”.

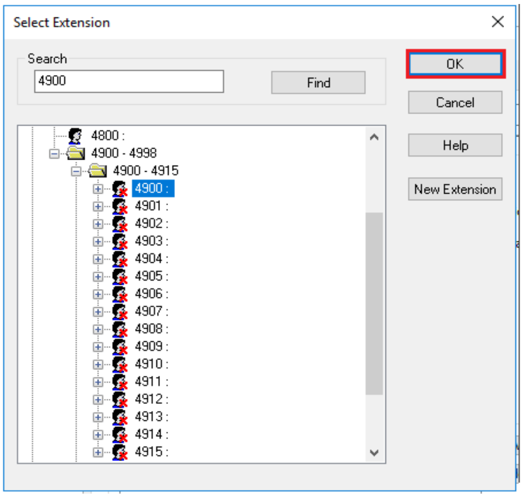
6. Select the Call Recording tab and uncheck both Recording Options. Then click **OK**.


Properties for Extension 4900 :

General | Forwarding | Address Groups | Call Recording

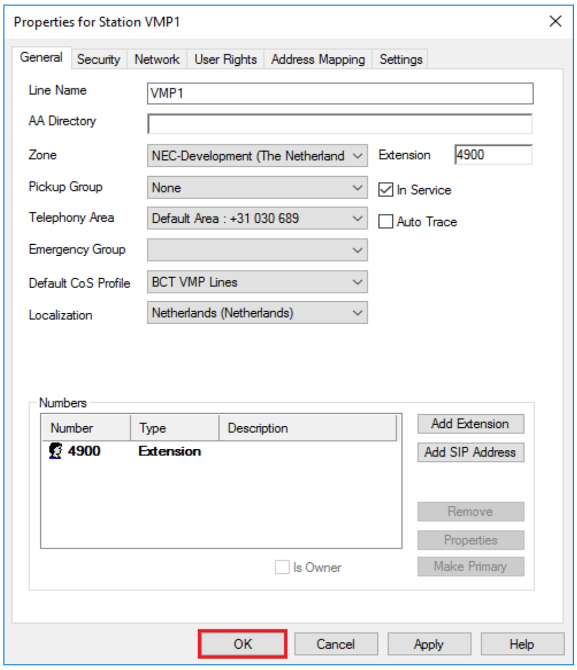
Recording Options
□ Allow Others to Record Your Calls
□ AutoRecord Your Calls

7. You then return to the "Select Extension" window. Select extension “4900” from the list and click **OK** twice.


Select Extension

Search: 4900

4800 :
4900 - 4998
4900 - 4915
4900 :
4901 :
4902 :
4903 :
4904 :
4905 :
4906 :
4907 :
4908 :
4909 :
4910 :
4911 :
4912 :
4913 :
4914 :
4915 :


Properties for Station VMP1

General | Security | Network | User Rights | Address Mapping | Settings

Line Name: VMP1
AA Directory:
Zone: NEC-Development (The Netherland
Extension: 4900
Pickup Group: None
☑ In Service
Telephony Area: Default Area : +31 030 689
□ Auto Trace
Emergency Group:
Default CoS Profile: BCT VMP Lines
Localization: Netherlands (Netherlands)

Numbers

Number	Type	Description
4900	Extension	

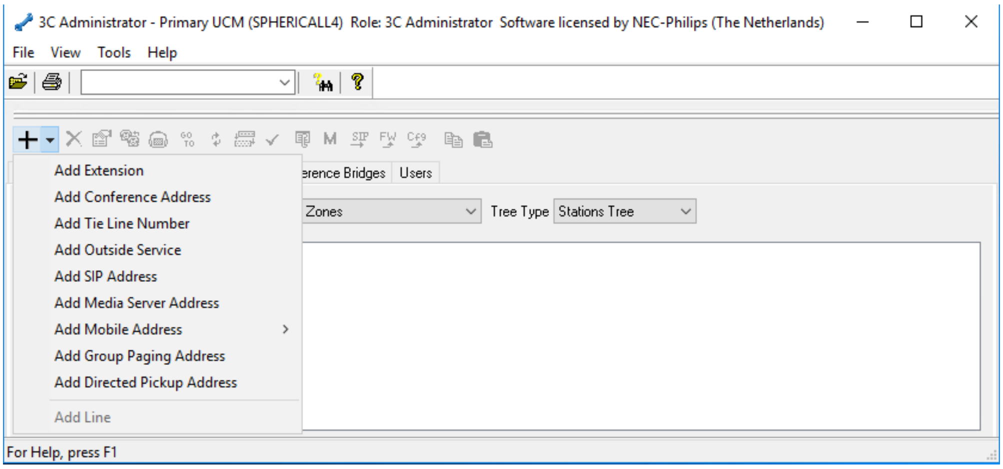
□ Is Owner

Note: *The red X shown on top of the user symbol indicates that this number will be hidden from any UNIVERGE 3C desktop.*

8. Repeat steps 2 – 6 for stations 4901, 4902, and 4903.

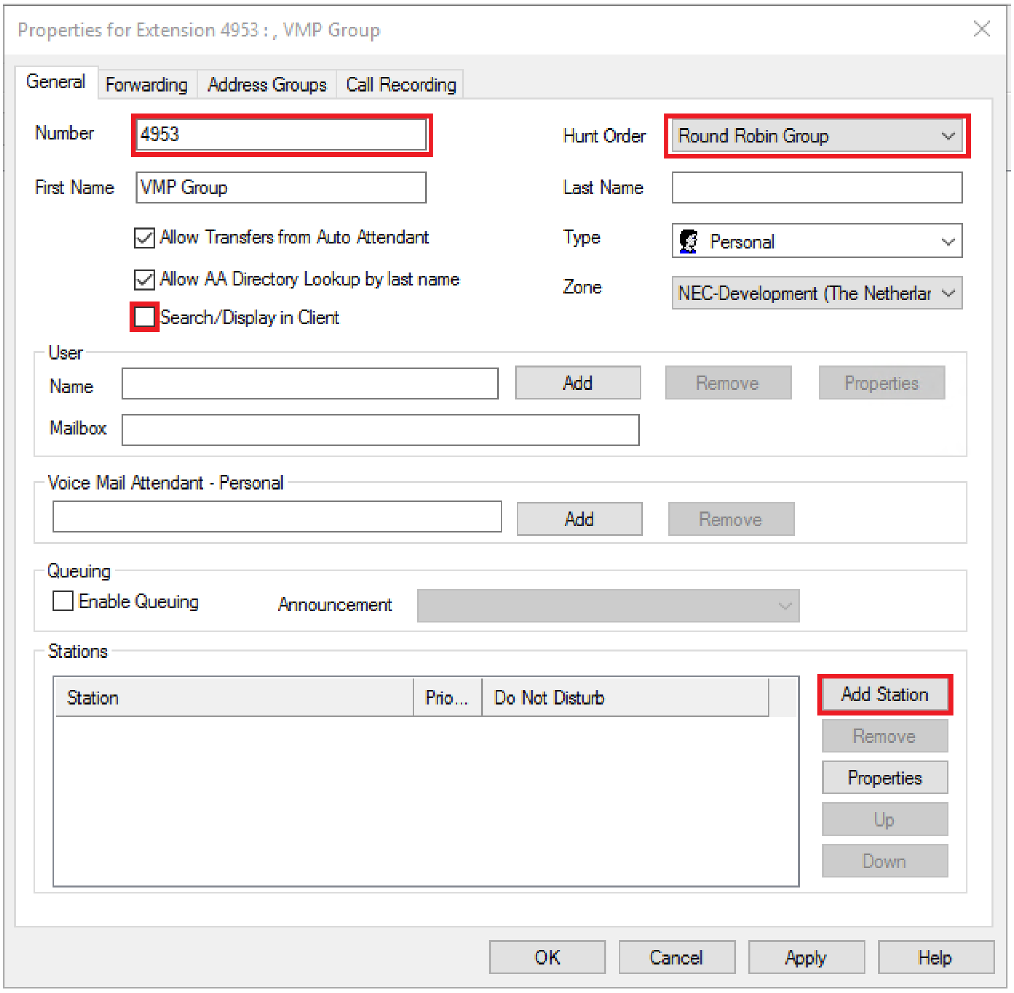
9. Create a Round Robin (RR) group extension to which the VMP lines will be added. In this example a Round Robin group will be created with 4 station members: 4900 to 4903. The RR group will become extension 4953.

10. Go to the "Number plan" tab and add a new extension by pressing the down arrow, right from the + icon on the UNIVERGE 3C Administrator toolbar.



11. Now the **Properties for new extension** window appears.

In the Number field, enter “4953”.
In the Hunt Order field select “Round Robin Group”.
Uncheck the checkbox for “Search/Display in Client”.
The First and Last Name fields are optional.



Properties for Extension 4953 : , VMP Group

Number: 4953

Hunt Order: Round Robin Group

First Name: VMP Group

Last Name:

☑ Allow Transfers from Auto Attendant

☑ Allow AA Directory Lookup by last name

☐ Search/Display in Client

Type: Personal

Zone: NEC-Development (The Netherlar

User

Name:

Mailbox:

Voice Mail Attendant - Personal

Queuing

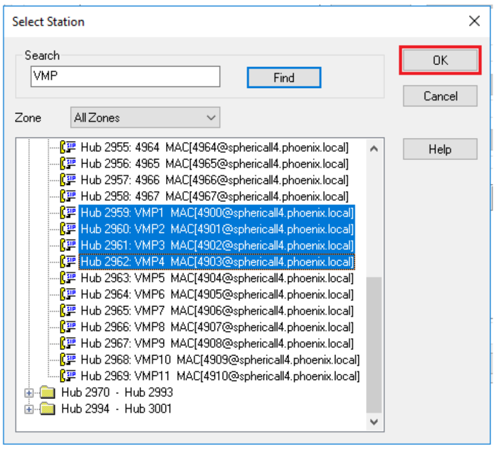
☐ Enable Queuing

Announcement:

Stations

Station	Prio...	Do Not Disturb

12. Click the **Add station** button. In the **Select Station** window select stations 4900 up to 4903 from the list (you can use the shift key to make a multiple selection) and click OK. The stations are now listed in the **Properties for new extension** window:

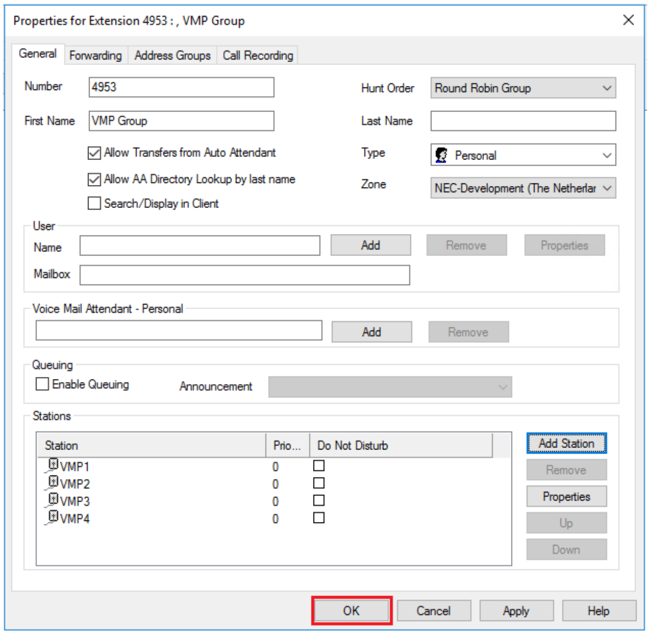


Select Station

Search: VMP

Zone: All Zones

```
Hub 2955: 4964  MAC[4964@sphericall4.phoenix.local]
Hub 2956: 4965  MAC[4965@sphericall4.phoenix.local]
Hub 2957: 4966  MAC[4966@sphericall4.phoenix.local]
Hub 2958: 4967  MAC[4967@sphericall4.phoenix.local]
Hub 2959: VMP1  MAC[4900@sphericall4.phoenix.local]
Hub 2960: VMP2  MAC[4901@sphericall4.phoenix.local]
Hub 2961: VMP3  MAC[4902@sphericall4.phoenix.local]
Hub 2962: VMP4  MAC[4903@sphericall4.phoenix.local]
Hub 2963: VMP5  MAC[4904@sphericall4.phoenix.local]
Hub 2964: VMP6  MAC[4905@sphericall4.phoenix.local]
Hub 2965: VMP7  MAC[4906@sphericall4.phoenix.local]
Hub 2966: VMP8  MAC[4907@sphericall4.phoenix.local]
Hub 2967: VMP9  MAC[4908@sphericall4.phoenix.local]
Hub 2968: VMP10  MAC[4909@sphericall4.phoenix.local]
Hub 2969: VMP11  MAC[4910@sphericall4.phoenix.local]
Hub 2970  -  Hub 2993
Hub 2994  -  Hub 3001
```



Properties for Extension 4953 : , VMP Group

Number: 4953

Hunt Order: Round Robin Group

First Name: VMP Group

Last Name:

☑ Allow Transfers from Auto Attendant

☑ Allow AA Directory Lookup by last name

☐ Search/Display in Client

Type: Personal

Zone: NEC-Development (The Netherlar

User

Name:

Mailbox:

Voice Mail Attendant - Personal

Queuing

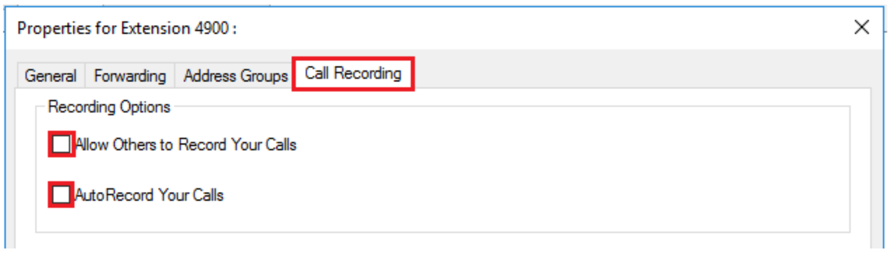
☐ Enable Queuing

Announcement:

Stations

Station	Prio...	Do Not Disturb
VMP1	0	☐
VMP2	0	☐
VMP3	0	☐
VMP4	0	☐

13. Select the Call Recording tab and uncheck both Recording Options. Then click **OK**.



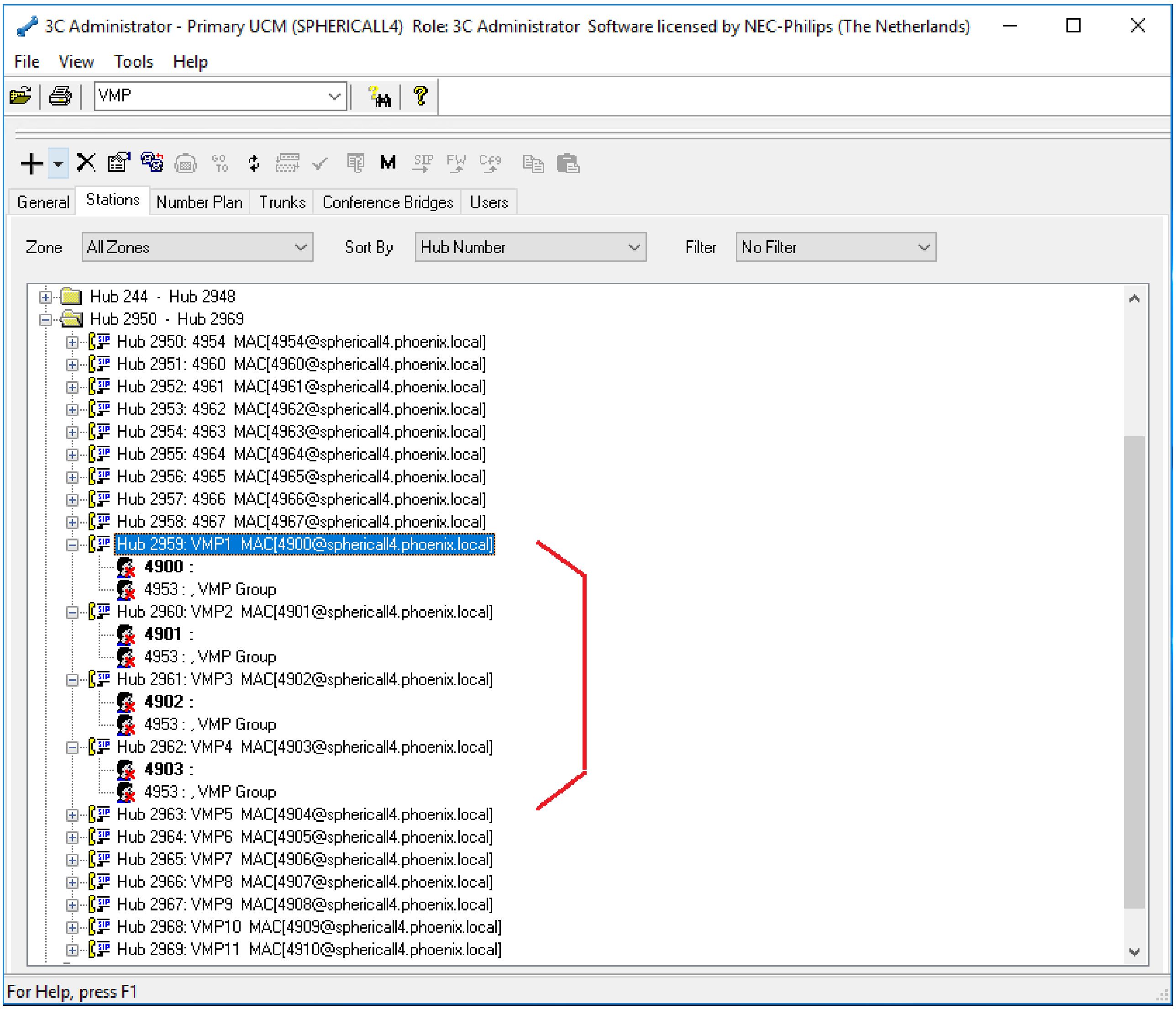
Properties for Extension 4900 :

Recording Options

□ Allow Others to Record Your Calls

□ AutoRecord Your Calls

14. In the “Stations” tab you can see that extensions have been added to the stations, as shown in the next figure:



3C Administrator - Primary UCM (SPHERICALL4) Role: 3C Administrator Software licensed by NEC-Philips (The Netherlands)

Zone: All Zones Sort By: Hub Number Filter: No Filter

```
Hub 244 - Hub 2948
Hub 2950 - Hub 2969
    Hub 2950: 4954  MAC[4954@sphericall4.phoenix.local]
    Hub 2951: 4960  MAC[4960@sphericall4.phoenix.local]
    Hub 2952: 4961  MAC[4961@sphericall4.phoenix.local]
    Hub 2953: 4962  MAC[4962@sphericall4.phoenix.local]
    Hub 2954: 4963  MAC[4963@sphericall4.phoenix.local]
    Hub 2955: 4964  MAC[4964@sphericall4.phoenix.local]
    Hub 2956: 4965  MAC[4965@sphericall4.phoenix.local]
    Hub 2957: 4966  MAC[4966@sphericall4.phoenix.local]
    Hub 2958: 4967  MAC[4967@sphericall4.phoenix.local]
    Hub 2959: VMP1  MAC[4900@sphericall4.phoenix.local]
        4900 :
        4953 : , VMP Group
    Hub 2960: VMP2  MAC[4901@sphericall4.phoenix.local]
        4901 :
        4953 : , VMP Group
    Hub 2961: VMP3  MAC[4902@sphericall4.phoenix.local]
        4902 :
        4953 : , VMP Group
    Hub 2962: VMP4  MAC[4903@sphericall4.phoenix.local]
        4903 :
        4953 : , VMP Group
    Hub 2963: VMP5  MAC[4904@sphericall4.phoenix.local]
    Hub 2964: VMP6  MAC[4905@sphericall4.phoenix.local]
    Hub 2965: VMP7  MAC[4906@sphericall4.phoenix.local]
    Hub 2966: VMP8  MAC[4907@sphericall4.phoenix.local]
    Hub 2967: VMP9  MAC[4908@sphericall4.phoenix.local]
    Hub 2968: VMP10  MAC[4909@sphericall4.phoenix.local]
    Hub 2969: VMP11  MAC[4910@sphericall4.phoenix.local]
```

For Help, press F1

4.6.4.7. Configure Contact Center Stations

In our example there are four numbers associated with the BCT Contact Center (see 4.6.1.5 Call Center configuration);

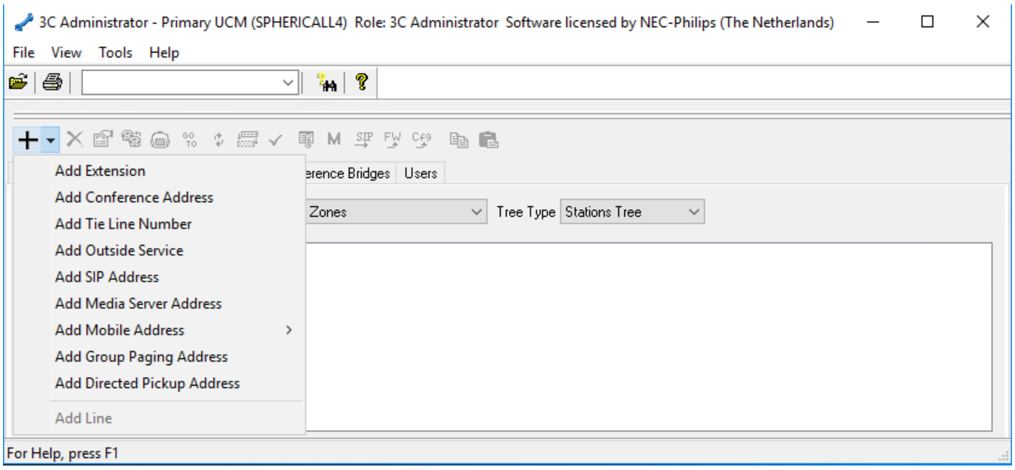
Agent Routing (Pilot Number):	4040
Agent Logon (for phone based agents):	4043
Prompt Recording:	4044
BCT Voicemail (Messagebox):	4954

These four numbers will all be attached to the same Station (4954), which was created by the UNIVERGE 3C SIP Line Configurator.

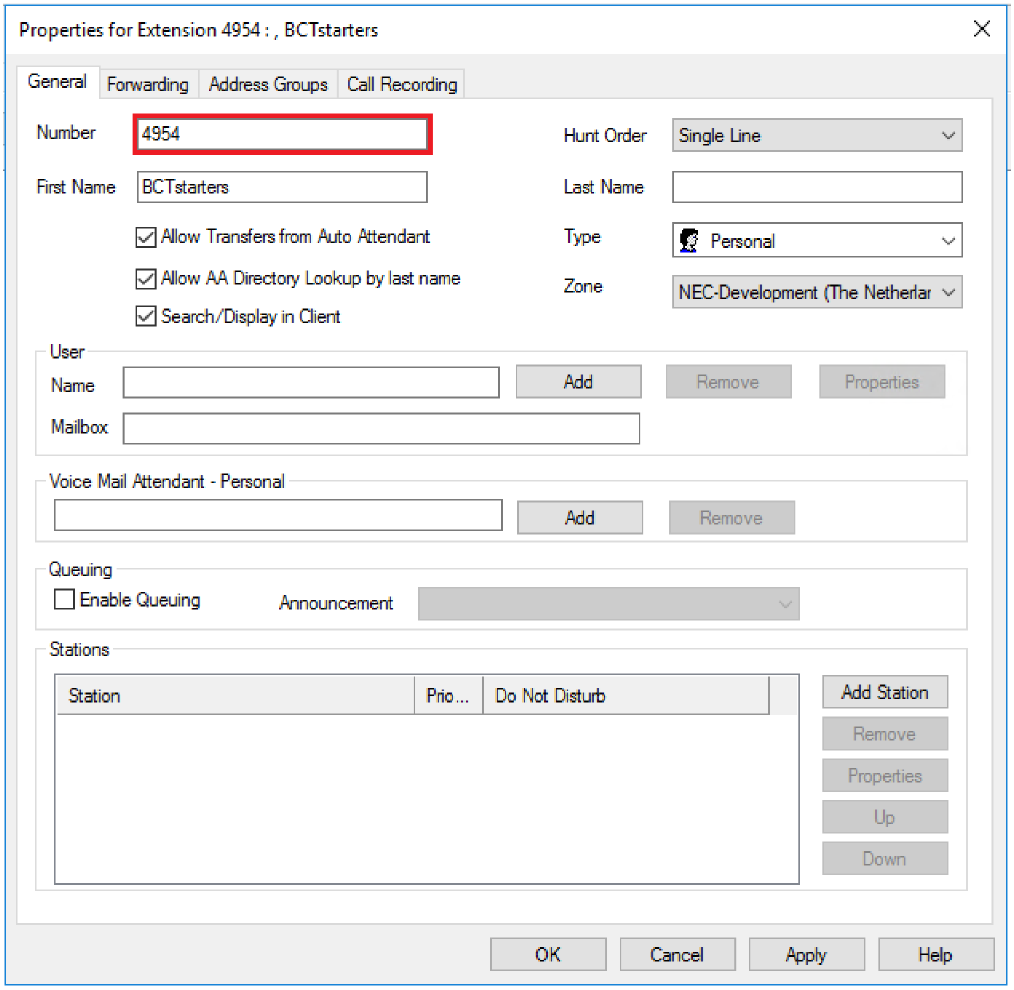
Note: *Numbers associated with the Contact Center cannot register on multi UNIVERGE 3C UCM servers, they must register at the same UNIVERGE 3C UCM server as BCT is connected to.*

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. Go to the "Number plan" tab and add a new extension by pressing the down arrow, right from the + icon on the UNIVERGE 3C Administrator toolbar.



3. Now the **Properties for new extension** window appears. In the Number field, enter “4954”. The First and Last Name fields are optional. Then click **OK**.



Properties for Extension 4954 : , BCTstarters

Number: 4954

First Name: BCTstarters

☑ Allow Transfers from Auto Attendant

☑ Allow AA Directory Lookup by last name

☑ Search/Display in Client

Hunt Order: Single Line

Last Name:

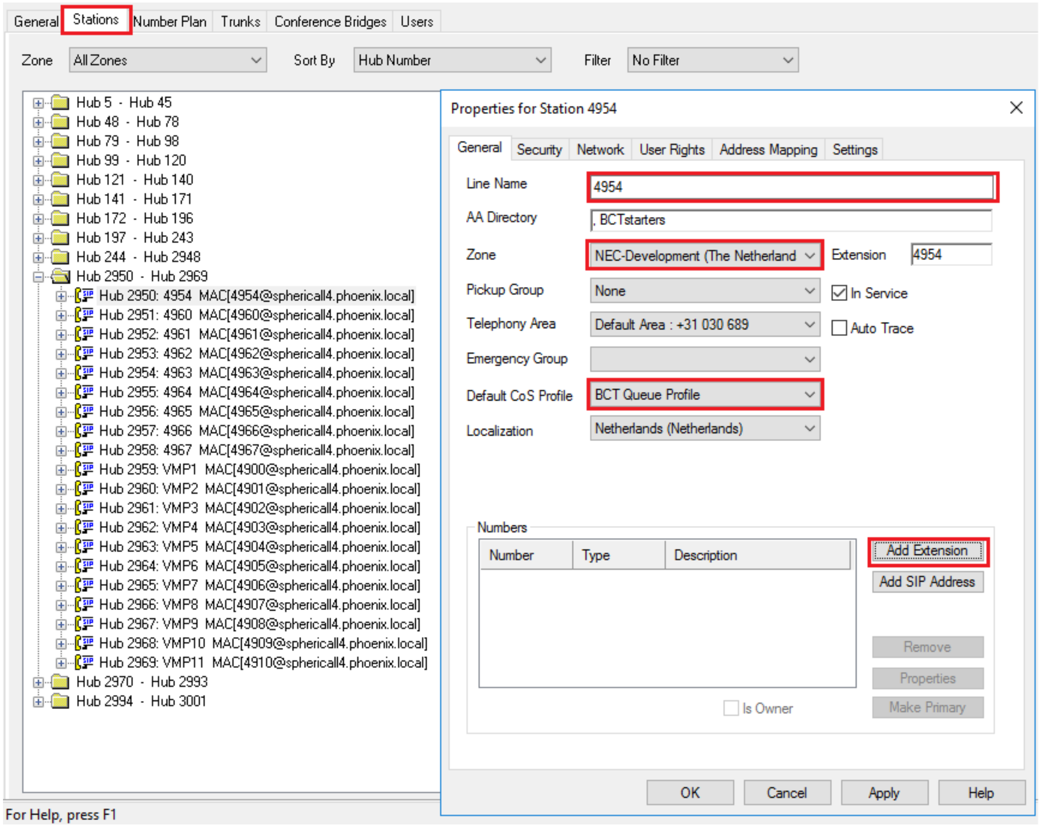
Type: Personal

Zone: NEC-Development (The Netherlar

☐ Enable Queuing

4. Repeat steps 2 and 3 to create extensions “4040”, “4043”, and “4044”.

5. Go to the “Stations” tab and look for the hub created for number 4954 which was added by the UNIVERGE 3C SIP Line Configurator (*see the example in Part Three*). Double-Click on the HUB for station “4954”.



Zone: All Zones | Sort By: Hub Number | Filter: No Filter

Hub 5 - Hub 45
Hub 48 - Hub 78
Hub 79 - Hub 98
Hub 99 - Hub 120
Hub 121 - Hub 140
Hub 141 - Hub 171
Hub 172 - Hub 196
Hub 197 - Hub 243
Hub 244 - Hub 2948
Hub 2950 - Hub 2969
Hub 2950: 4954 MAC[4954@sphericall4.phoenix.local]
Hub 2951: 4960 MAC[4960@sphericall4.phoenix.local]
Hub 2952: 4961 MAC[4961@sphericall4.phoenix.local]
Hub 2953: 4962 MAC[4962@sphericall4.phoenix.local]
Hub 2954: 4963 MAC[4963@sphericall4.phoenix.local]
Hub 2955: 4964 MAC[4964@sphericall4.phoenix.local]
Hub 2956: 4965 MAC[4965@sphericall4.phoenix.local]
Hub 2957: 4966 MAC[4966@sphericall4.phoenix.local]
Hub 2958: 4967 MAC[4967@sphericall4.phoenix.local]
Hub 2959: VMP1 MAC[4900@sphericall4.phoenix.local]
Hub 2960: VMP2 MAC[4901@sphericall4.phoenix.local]
Hub 2961: VMP3 MAC[4902@sphericall4.phoenix.local]
Hub 2962: VMP4 MAC[4903@sphericall4.phoenix.local]
Hub 2963: VMP5 MAC[4904@sphericall4.phoenix.local]
Hub 2964: VMP6 MAC[4905@sphericall4.phoenix.local]
Hub 2965: VMP7 MAC[4906@sphericall4.phoenix.local]
Hub 2966: VMP8 MAC[4907@sphericall4.phoenix.local]
Hub 2967: VMP9 MAC[4908@sphericall4.phoenix.local]
Hub 2968: VMP10 MAC[4909@sphericall4.phoenix.local]
Hub 2969: VMP11 MAC[4910@sphericall4.phoenix.local]
Hub 2970 - Hub 2993
Hub 2994 - Hub 3001

Properties for Station 4954

Line Name: 4954
AA Directory: , BCTstarters
Zone: NEC-Development (The Netherland
Extension: 4954
Pickup Group: None
☑ In Service
Telephony Area: Default Area : +31 030 689
☐ Auto Trace
Emergency Group:
Default CoS Profile: BCT Queue Profile
Localization: Netherlands (Netherlands)

Numbers

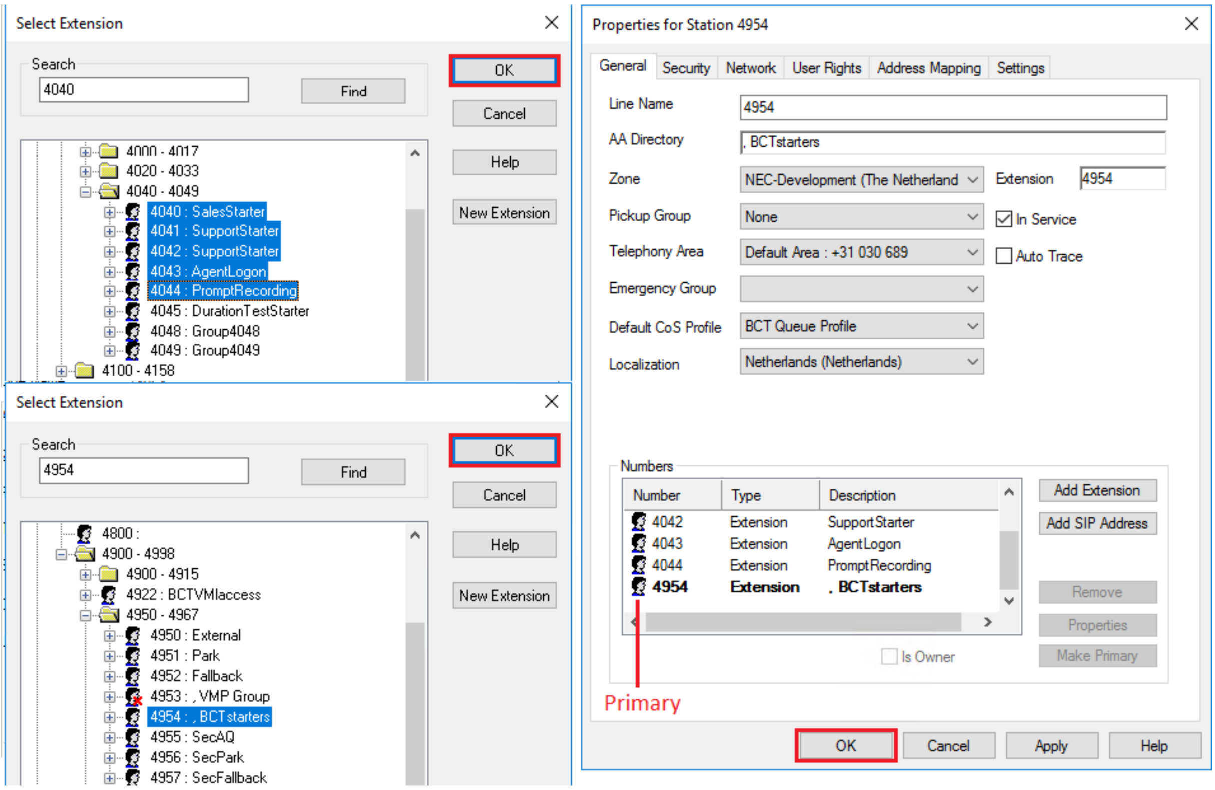
Number	Type	Description

☐ Is Owner

6. In the Properties for Station window, choose the General tab and enter the following;

Line Name:	Optional – Enter a descriptive name such as “4954”
Zone:	Choose the zone from the pull-down menu
Pickup Group:	Leave default “None”
Telephony Area:	Leave default or choose a new one from the pull-down menu
Emergency Group:	Leave blank
Default CoS Profile:	Choose “BCT Queue Profile” from the pull-down menu (from section 4.3)
Localization:	Select your location or leave default “Netherlands (Netherlands)”

7. Now you must assign extension numbers from steps 2 and 3 to this station. Click **Add Extension**.


Select Extension

Search: 4040

- 4000 - 4017
- 4020 - 4033
- 4040 - 4049
  - 4040 : SalesStarter
  - 4041 : SupportStarter
  - 4042 : SupportStarter
  - 4043 : AgentLogon
  - 4044 : PromptRecording
  - 4045 : DurationTestStarter
  - 4048 : Group4048
  - 4049 : Group4049
- 4100 - 4158

Select Extension

Search: 4954

- 4800 :
- 4900 - 4998
  - 4900 - 4915
  - 4922 : BCTVMIaccess
  - 4950 - 4967
    - 4950 : External
    - 4951 : Park
    - 4952 : Fallback
    - 4953 : , VMP Group
    - 4954 : , BCTstarters
    - 4955 : SecAQ
    - 4956 : SecPark
    - 4957 : SecFallback

Properties for Station 4954

Line Name	4954
AA Directory	, BCTstarters
Zone	NEC-Development (The Netherland
Extension	4954
Pickup Group	None
☑ In Service	
Telephony Area	Default Area : +31 030 689
☐ Auto Trace	
Emergency Group	
Default CoS Profile	BCT Queue Profile
Localization	Netherlands (Netherlands)

Numbers

Number	Type	Description
4042	Extension	SupportStarter
4043	Extension	AgentLogon
4044	Extension	PromptRecording
4954	**Extension**	**, BCTstarters**

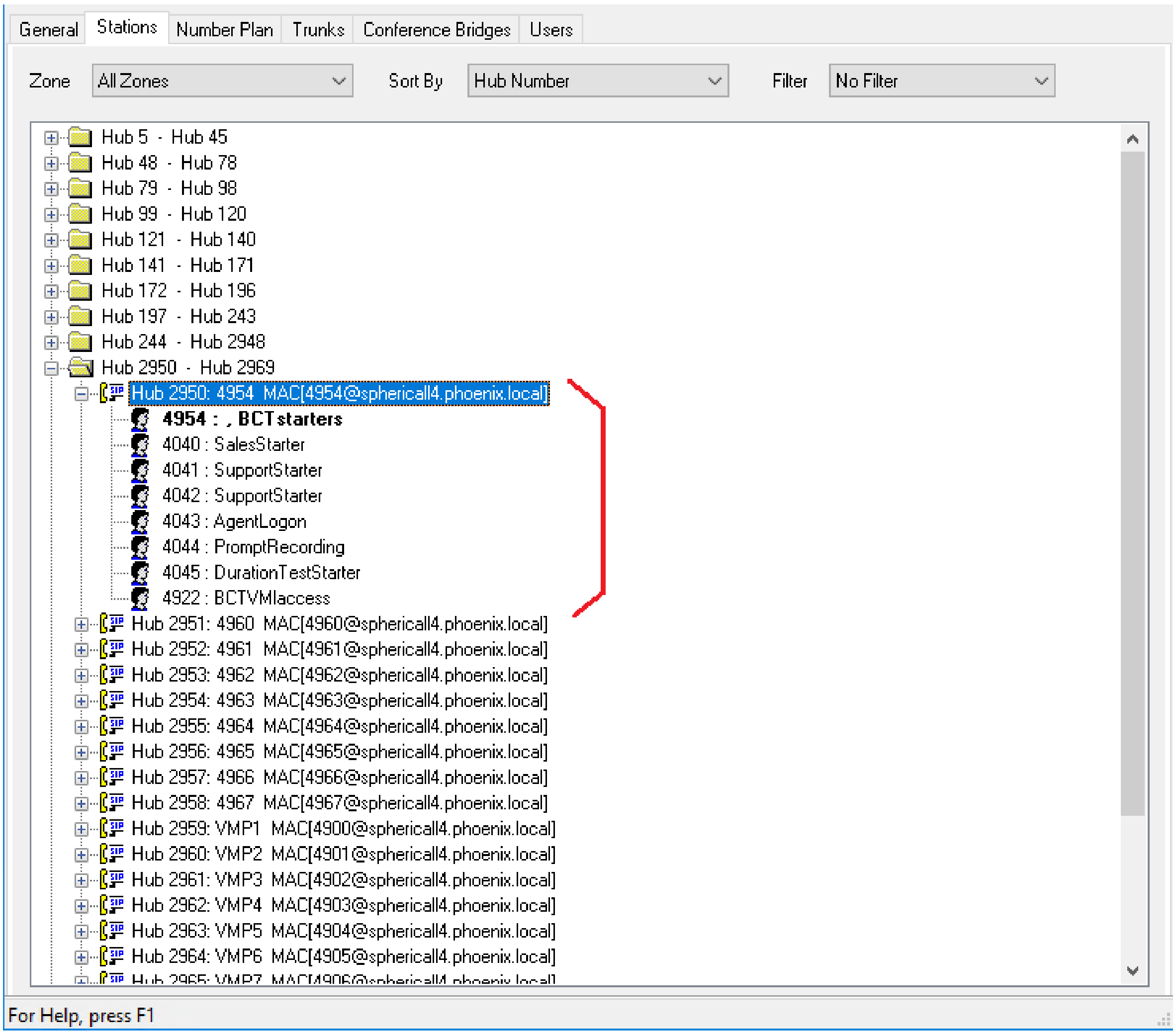
☐ Is Owner

Primary

8. In the **Select Extension** window select extensions 4040, 4043, 4044, and 4954 from the list (you can use the Ctrl key to make a multiple selection) and click OK. The extensions are now listed in the **Properties for new station** window; click **OK**.

Note: *Extension 4954 should be in* ***Bold*** *type. If it is not, click 4954 once to highlight it, and then click the "Make Primary" button.*

9. In the "Stations" tab you can see that the extensions have been added to the station, as shown in the next figure:



Zone: All Zones
Sort By: Hub Number
Filter: No Filter

```
⊞ Hub 5 - Hub 45
⊞ Hub 48 - Hub 78
⊞ Hub 79 - Hub 98
⊞ Hub 99 - Hub 120
⊞ Hub 121 - Hub 140
⊞ Hub 141 - Hub 171
⊞ Hub 172 - Hub 196
⊞ Hub 197 - Hub 243
⊞ Hub 244 - Hub 2948
⊟ Hub 2950 - Hub 2969
    ⊟ Hub 2950: 4954  MAC[4954@sphericall4.phoenix.local]
        4954 : , BCT starters
        4040 : SalesStarter
        4041 : SupportStarter
        4042 : SupportStarter
        4043 : AgentLogon
        4044 : PromptRecording
        4045 : DurationTestStarter
        4922 : BCTVMIaccess
    ⊞ Hub 2951: 4960  MAC[4960@sphericall4.phoenix.local]
    ⊞ Hub 2952: 4961  MAC[4961@sphericall4.phoenix.local]
    ⊞ Hub 2953: 4962  MAC[4962@sphericall4.phoenix.local]
    ⊞ Hub 2954: 4963  MAC[4963@sphericall4.phoenix.local]
    ⊞ Hub 2955: 4964  MAC[4964@sphericall4.phoenix.local]
    ⊞ Hub 2956: 4965  MAC[4965@sphericall4.phoenix.local]
    ⊞ Hub 2957: 4966  MAC[4966@sphericall4.phoenix.local]
    ⊞ Hub 2958: 4967  MAC[4967@sphericall4.phoenix.local]
    ⊞ Hub 2959: VMP1  MAC[4900@sphericall4.phoenix.local]
    ⊞ Hub 2960: VMP2  MAC[4901@sphericall4.phoenix.local]
    ⊞ Hub 2961: VMP3  MAC[4902@sphericall4.phoenix.local]
    ⊞ Hub 2962: VMP4  MAC[4903@sphericall4.phoenix.local]
    ⊞ Hub 2963: VMP5  MAC[4904@sphericall4.phoenix.local]
    ⊞ Hub 2964: VMP6  MAC[4905@sphericall4.phoenix.local]
    ⊞ Hub 2965: VMP7  MAC[4906@sphericall4.phoenix.local]
```

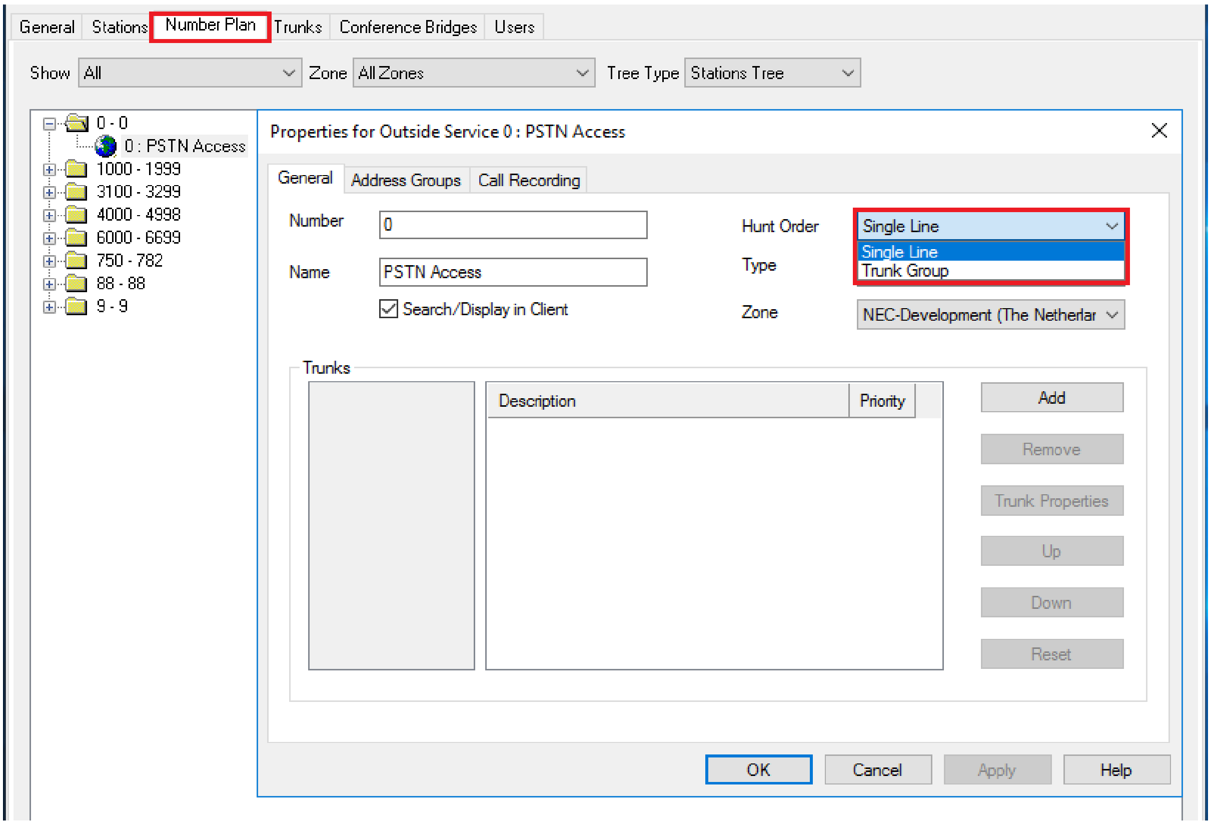
For Help, press F1

4.6.4.8. Outside Service Hunt Order

Set the Hunt Order of Outside Service (i.e. the trunk access code) to Single Line.

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. Select the “Numbering Plan” tab. Double-click on the Outside Service access number (typically “0”).



Show: All
Zone: All Zones
Tree Type: Stations Tree

Properties for Outside Service 0 : PSTN Access

Number: 0
Name: PSTN Access
☑ Search/Display in Client
Hunt Order: Single Line
Zone: NEC-Development (The Netherlar

3. Set the Hunt Order to “Single Line” then click OK.

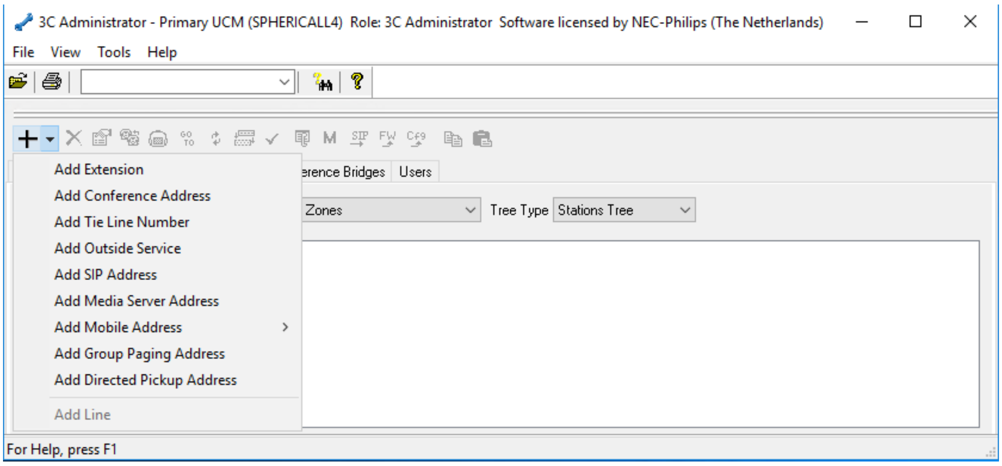
4.6.4.9. Configure CTIuser

The user “CTIuser” was created in Active Directory (see 4.6.2 Active Directory), now it must be added to UNIVERGE 3C. Note that “CTIuser” requires a Dummy Extension. This extension will never be called so can be any number and does not have to be a valid dialable number. For this example, “1000” will be used.

Caution: When Open Numbering Plan is enabled, each zone needs an ‘own’ “CTIuser” (see 4.6.4.13 Configuring Open Numbering Plan)

1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

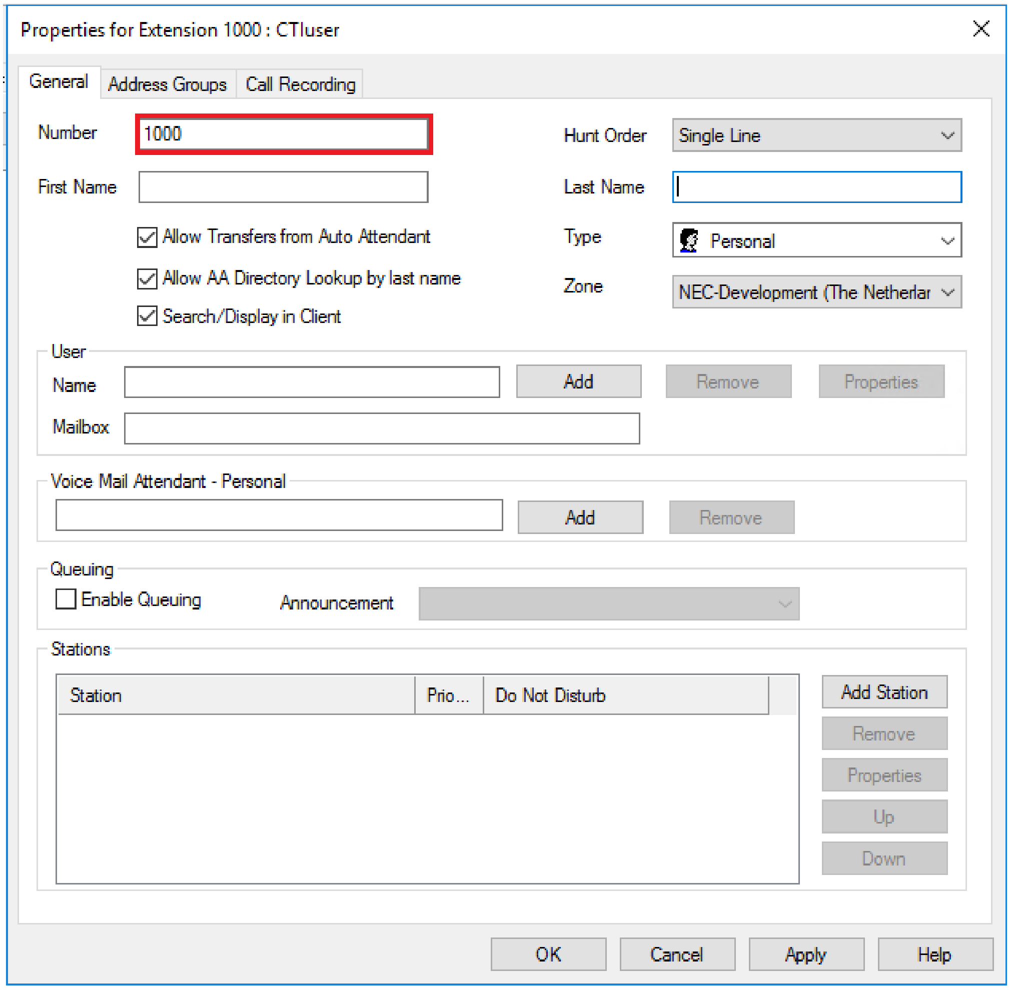
2. To create a Dummy Extension, go to the "Number plan" tab and add a new extension by pressing the down arrow, right from the + icon on the UNIVERGE 3C Administrator toolbar.


3C Administrator - Primary UCM (SPHERICALL4) Role: 3C Administrator Software licensed by NEC-Philips (The Netherlands)

Tree Type: Stations Tree

For Help, press F1

3. Now the **Properties for new extension** window appears. In the Number field, enter “1000” then click **OK**.


Properties for Extension 1000 : CTIuser

Number: 1000

First Name:

Hunt Order: Single Line

Last Name:

Type: Personal

Zone: NEC-Development (The Netherlar

☑ Allow Transfers from Auto Attendant

☑ Allow AA Directory Lookup by last name

☑ Search/Display in Client

User

Name:

Mailbox:

Voice Mail Attendant - Personal

Queuing

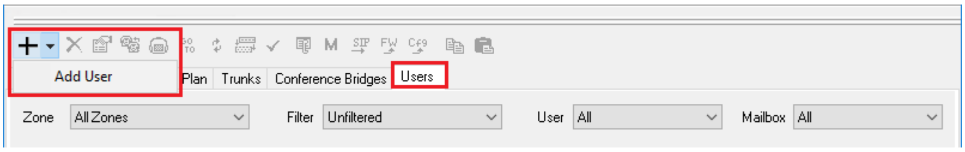
☐ Enable Queuing

Announcement:

Stations

Station	Prio...	Do Not Disturb

4. To add “CTIuser” to UNIVERGE 3C, go to the "Users" tab and add a new user by pressing the down arrow, right from the + icon on the UNIVERGE 3C Administrator toolbar.

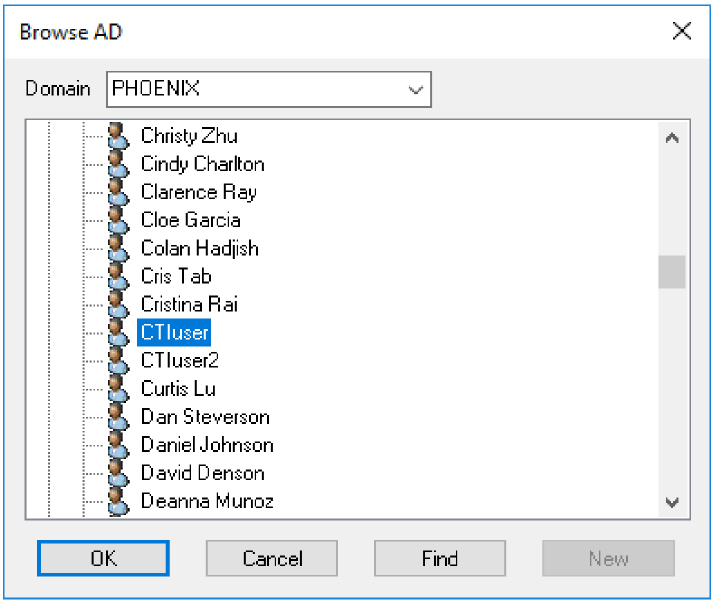

Zone: All Zones

Filter: Unfiltered

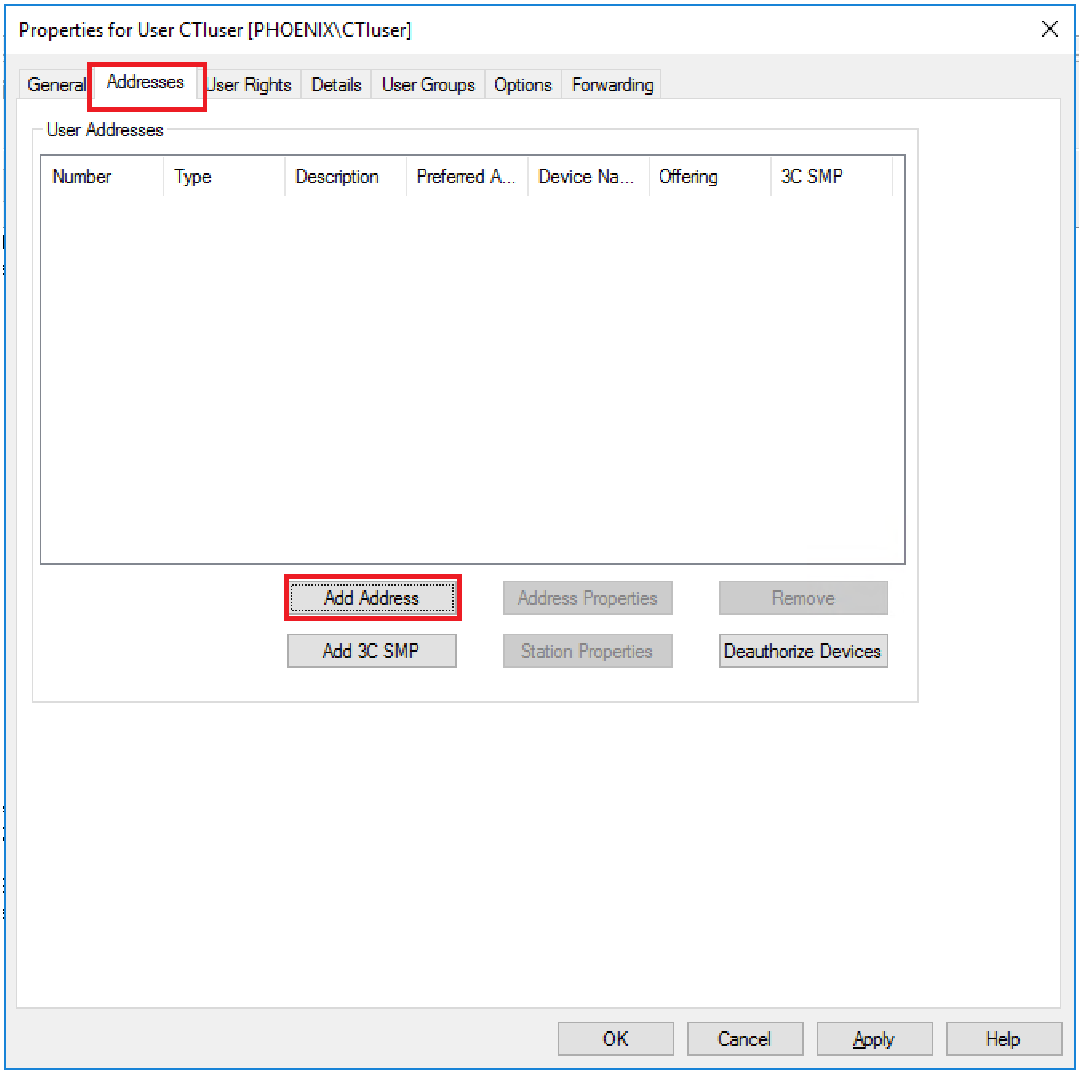
User: All

Mailbox: All

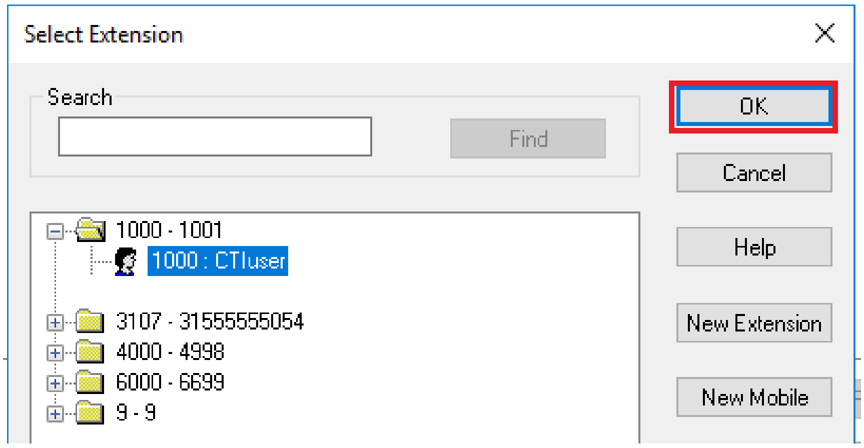
5. In the **Browse AD** window, expand the Active Directory Container (folder) where “CTIuser” was created. Select “CTIuser” and click OK.



6. In the tab Addressess of the **Properties for User** window, click **Add Address**.



7. In the **Select Extension** window, select “1000” then click **OK**.



Select Extension

Search

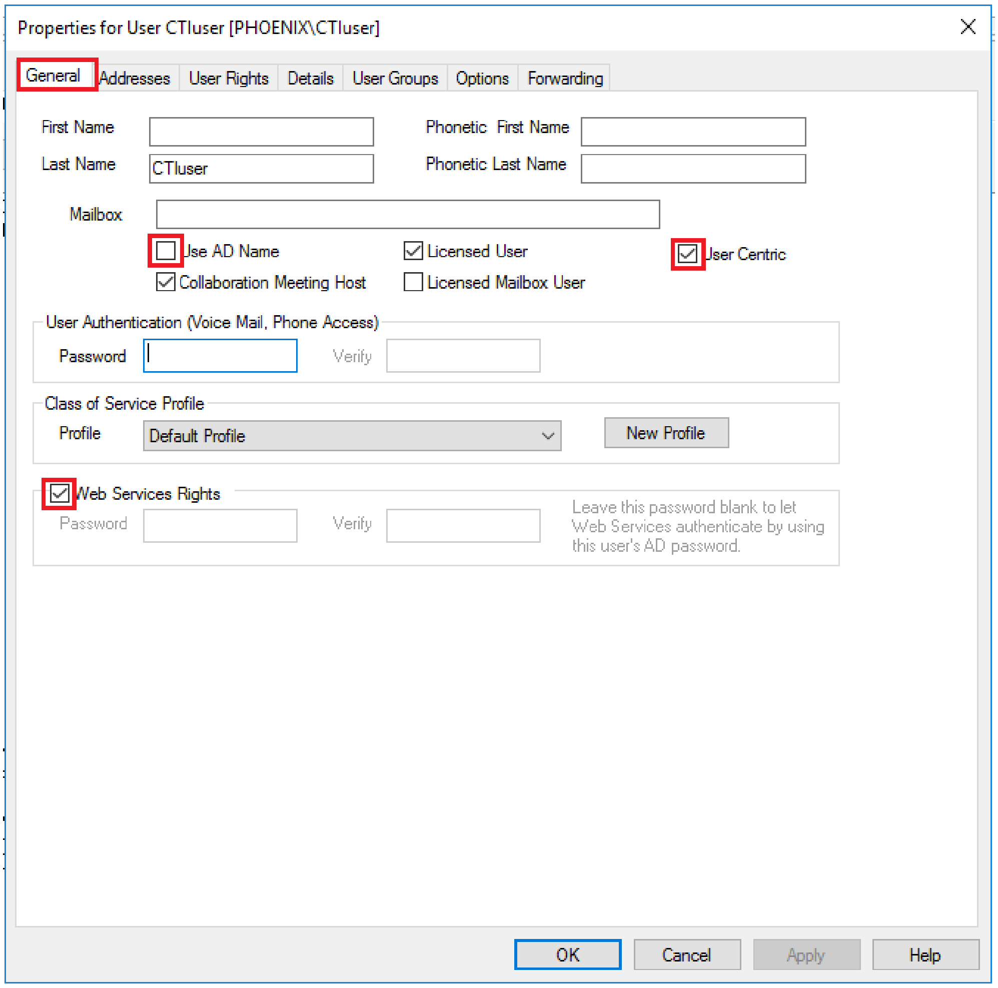
1000 - 1001
- 1000 : CTIuser

3107 - 31555555054
4000 - 4998
6000 - 6699
9 - 9

8. In the tab General of the **Properties for User** window, set the following options:

Use AD Name = Unchecked
User Centric = Checked
Web Services Rights = Checked

Other options should remain default. Click **Apply**.



Properties for User CTIuser [PHOENIX\CTIuser]

First Name:
Last Name: CTIuser
Phonetic First Name:
Phonetic Last Name:
Mailbox:

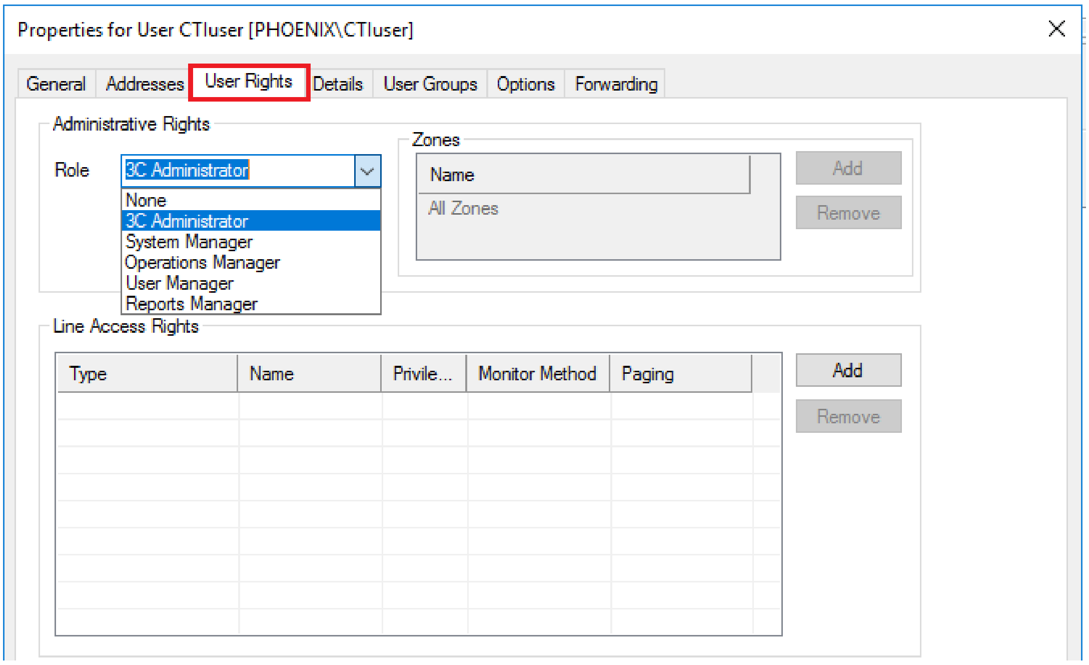
□ Use AD Name
☑ Licensed User
☑ User Centric
☑ Collaboration Meeting Host
□ Licensed Mailbox User

User Authentication (Voice Mail, Phone Access)
Password:
Verify:

Class of Service Profile
Profile: Default Profile

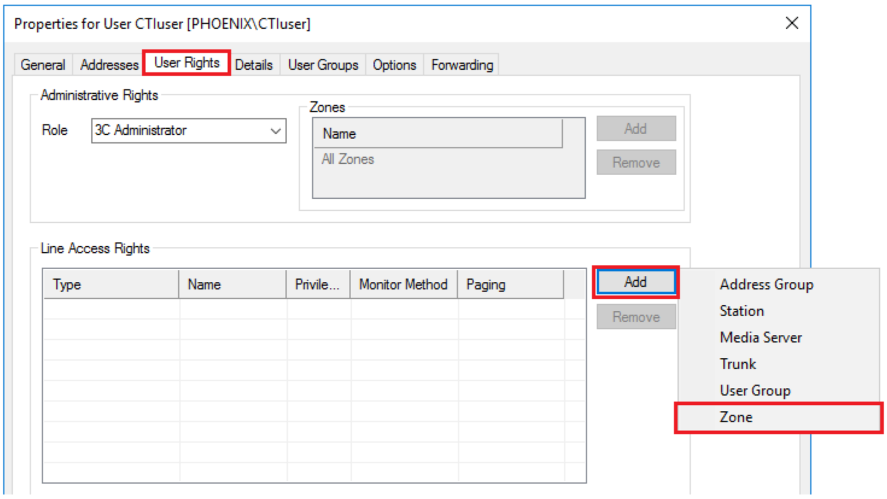
☑ Web Services Rights
Password:
Verify:
Leave this password blank to let Web Services authenticate by using this user's AD password.

9. Select the “User Rights” tab. In section Administrative Rights select Role 3C Administrator.



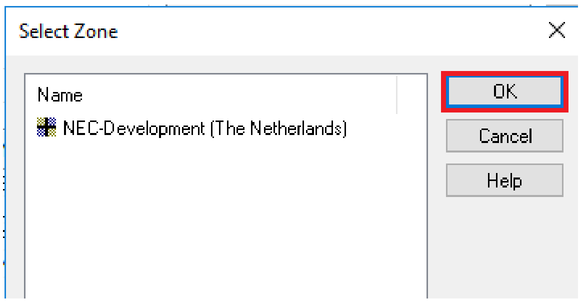
Properties for User CTIuser [PHOENIX\CTIuser]

10. Select the “User Rights” tab. Click Add and select “Zone”.



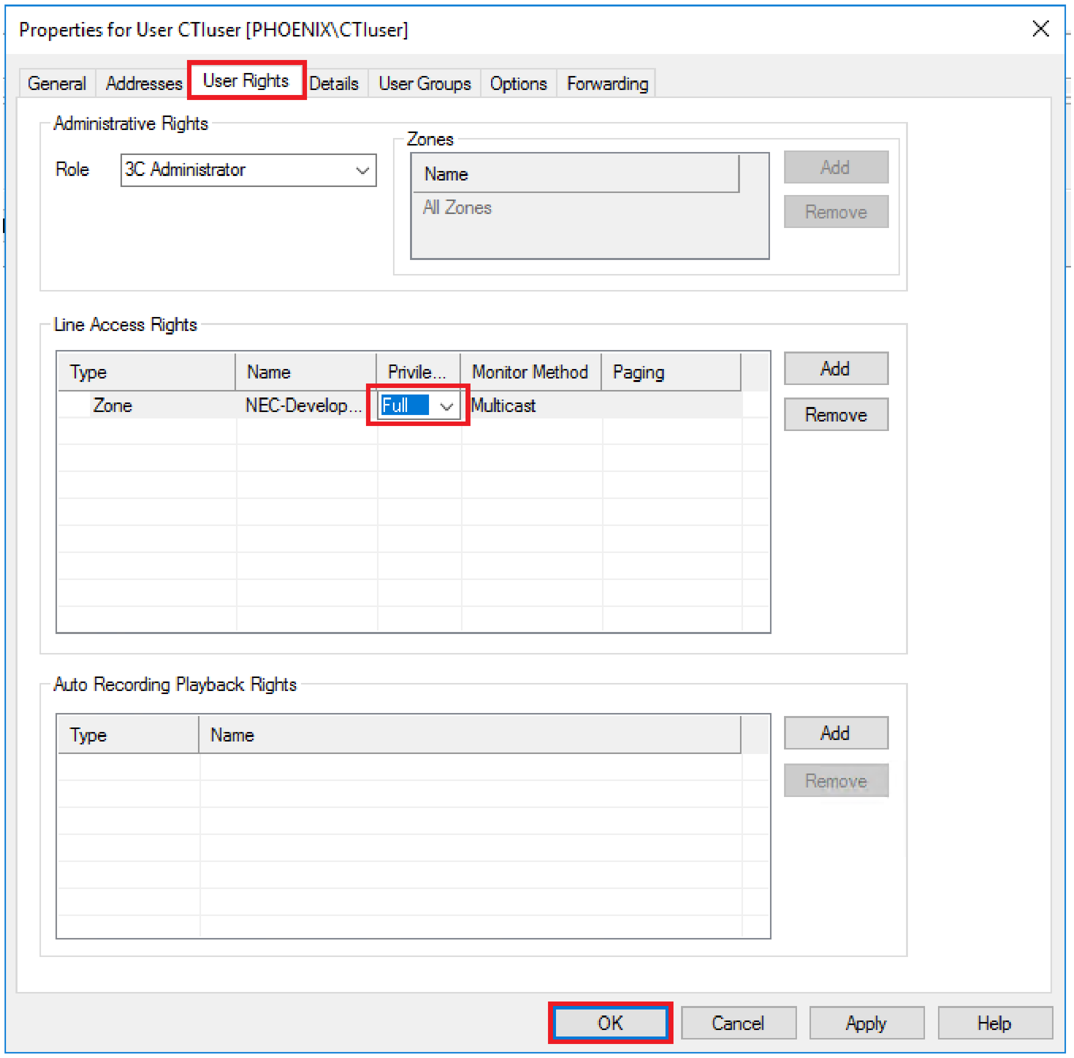
Properties for User CTIuser [PHOENIX\CTIuser]

11. In the **Select Zone** window, choose the Zone(s) in which BCT resides and click **OK**. Select in BCT which zones should in the company and in the external directory.



Select Zone

12. Set the Zone “Privilege” to “Full” then click **OK**.



Properties for User CTIuser [PHOENIX\CTIuser]

Administrative Rights

Role: 3C Administrator

Zones

Name
All Zones

Line Access Rights

Type	Name	Privile...	Monitor Method	Paging
Zone	NEC-Develop...	Full	Multicast	

Auto Recording Playback Rights

Type	Name

4.6.4.10. Configure BCT users

The following steps must be applied to any User which will be a BCT Operator or BCT Agent.

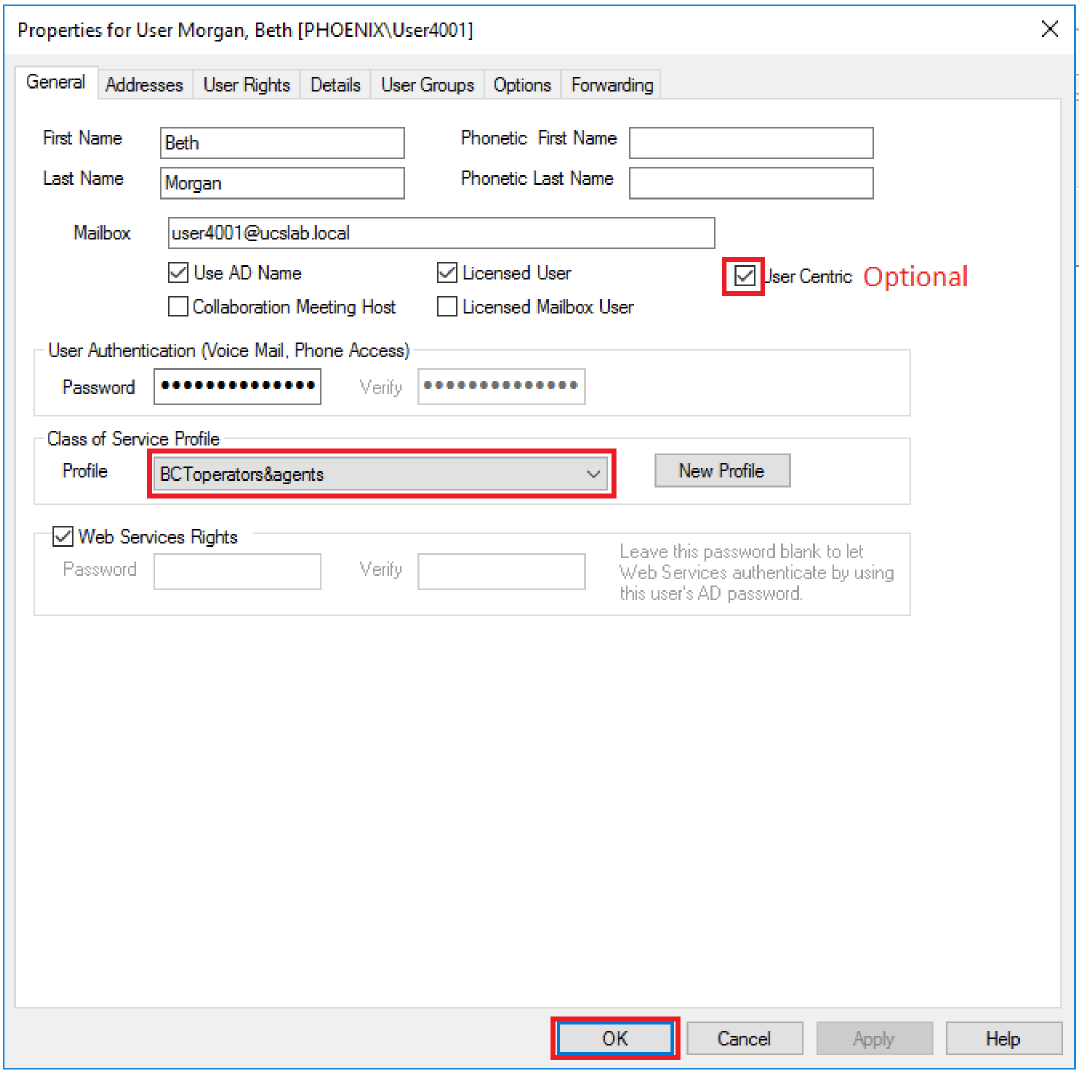
1. Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.

2. Go to the “Users” tab and double-click the user to open the **Properties for User** window. Set the following and then click **Apply**;

User Centric: Optional: either Address Centric or User Centric can be used. (*BCT 6.0 and higher*)

Preferred: A User can be associated with multiple addresses, but one number must be set as the “Preferred” address.

Class of Service Profile: Set to BCT Operators & Agents Users (which was created in 4.6.4.3 Class of Service)



Properties for User Morgan, Beth [PHOENIX\User4001]

First Name: Beth

Last Name: Morgan

Phonetic First Name:

Phonetic Last Name:

Mailbox: user4001@ucslab.local

☑ Use AD Name ☑ Licensed User ☑ User Centric Optional

☐ Collaboration Meeting Host ☐ Licensed Mailbox User

User Authentication (Voice Mail, Phone Access)

Password: •••••••••••••• Verify: ••••••••••••••

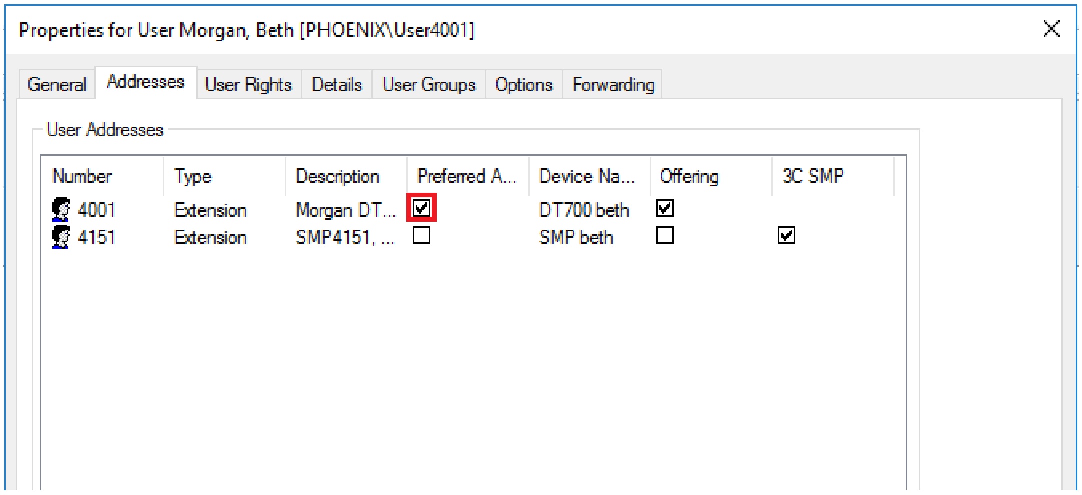
Class of Service Profile

Profile: BCToperators&agents

☑ Web Services Rights

Password: Verify:

Leave this password blank to let Web Services authenticate by using this user's AD password.

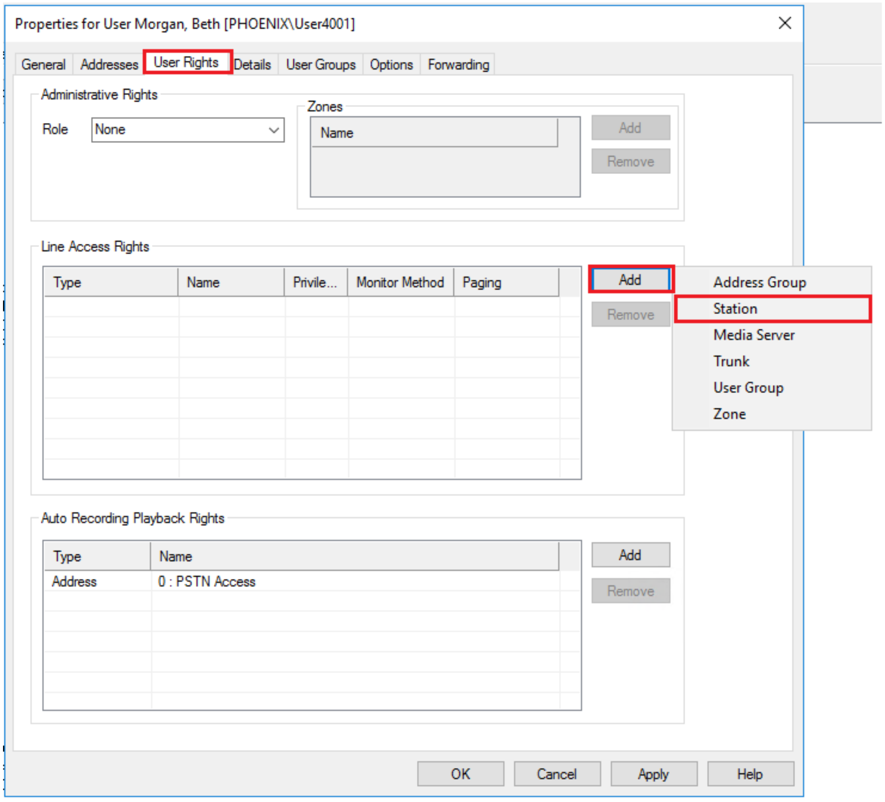


Properties for User Morgan, Beth [PHOENIX\User4001]

User Addresses

Number	Type	Description	Preferred A...	Device Na...	Offering	3C SMP
4001	Extension	Morgan DT...	☑	DT700 beth	☑	
4151	Extension	SMP4151, ...	☐	SMP beth	☐	☑

3. Go to the “User Rights” tab. Click **Add** and select Station.

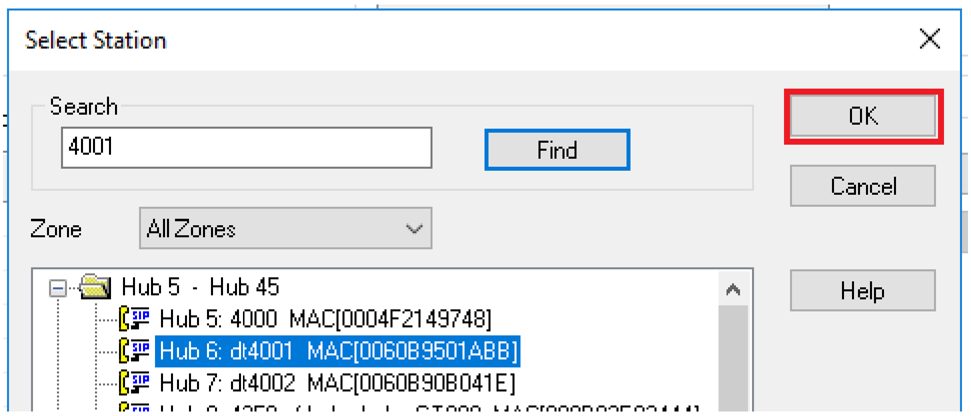


Properties for User Morgan, Beth [PHOENIX\User4001]

Role: None

Type	Name
Address	0 : PSTN Access

4. In the **Select Station** window, select the Hub for this user and click **OK**.

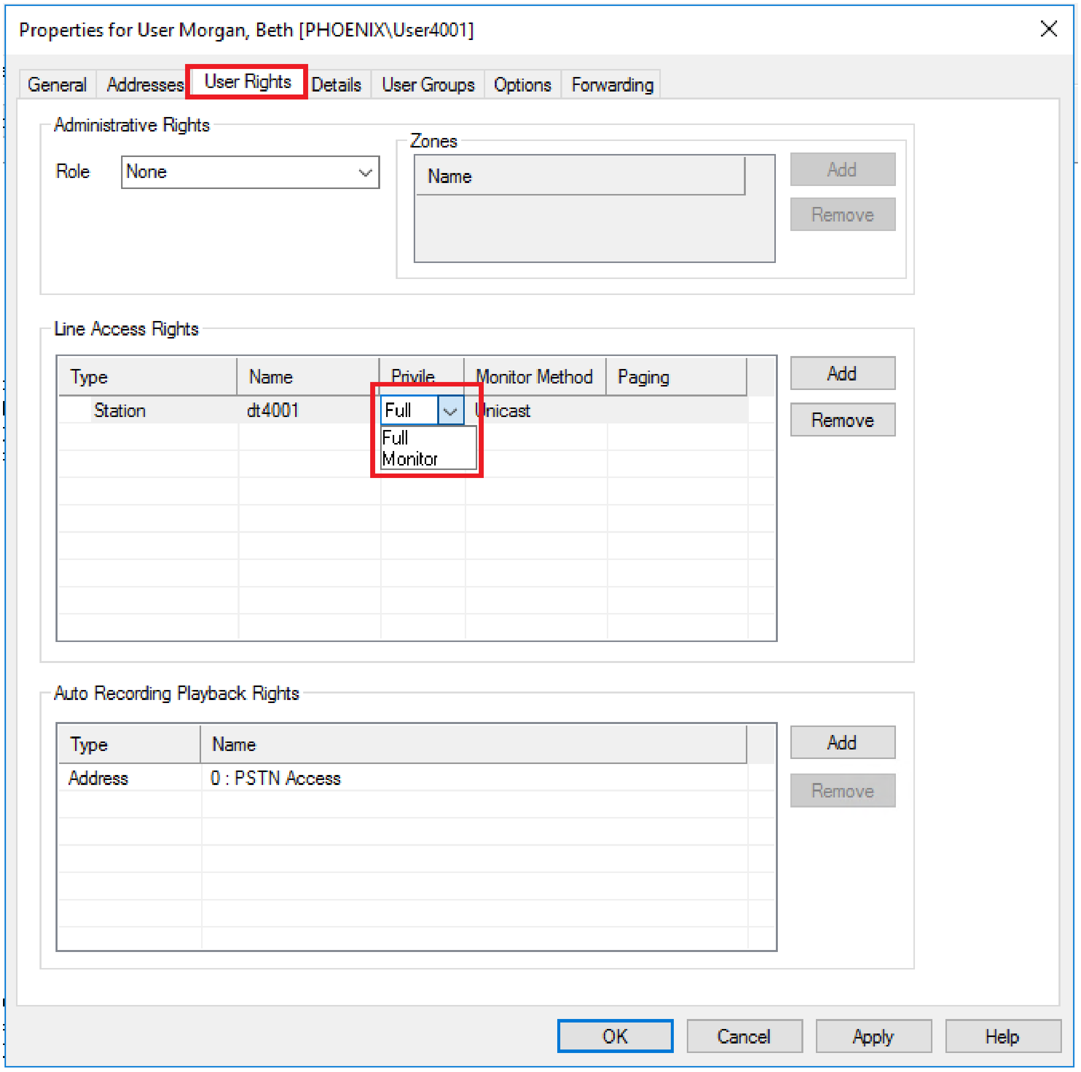


Search: 4001

Zone: All Zones

```
Hub 5 - Hub 45
    Hub 5: 4000  MAC[0004F2149748]
    Hub 6: dt4001  MAC[0060B9501ABB]
    Hub 7: dt4002  MAC[0060B90B041E]
```

5. Set “Privilege” to “Full” for the Station. Then click **OK**.



Properties for User Morgan, Beth [PHOENIX\User4001]

Administrative Rights

Role: None

Zones

Name

Line Access Rights

Type	Name	Privile	Monitor Method	Paging
Station	dt4001	Full	Unicast	

Auto Recording Playback Rights

Type	Name
Address	0 : PSTN Access

6. Repeat steps 2 through 5 for all Users who will be BCT Operators or BCT Agents.

7. To configure Precense status and Instant Messaging between BCT Operator / BCT Agents and Univerge 3C UC Clients see Appendix N-3 – Configure Presence & Instant Messaging between UNIVERGE 3C and BCT

4.6.4.11. Add SIP User Agent for DECT phones

When it is necessary to add additional User Agent profiles for DECT Phones, make sure that the Agent Description starts with “NEC IP DECT Handset”, the remaining characters are not considered by BCT. Only then BCT will recognise that it is a DECT phone.

4.6.4.12. Configuring Outbound Caller ID

When Outbound Caller Id is configured (see BCT Supervisor Dashboard) depending on the Caller Id digits to be sent also configuration in the UNIVERGE 3C system is needed:

1. When the Outbound Caller ID (last X digits) are already part of the internal number plan (DID Mapping), no special configuration is needed

2. When the Outbound Caller ID (last X digits) are not part of the internal number plan, add a dummy address in number plan using UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC.

3. When the Outbound Caller ID should contain more digits than the internal number plan (e.g. 0800 1234 5678):

   - Start the UNIVERGE 3C Administrator on the UNIVERGE 3C Manager PC, either from the start menu or from the desktop.
   - Select the General tab and expand
   - Select Mapping List > DID Mapping
   - Add a new Mapping list (e.g. BCT CID List):
   - Add a new mapping in the list:
     i. Address-type: Extension
     ii. Number: The required number (e.g. 080012345678)
     iii. Extension/Rule: a dummy address outside the existing internal number plan (e.g. 5000), note that this number may not conflict with an existing address in the system.
   - Add the new Mapping List to the Inward Routing Mapping of the trunk involved
   - Using the dummy address (e.g. 5000) in the BCT Supervisor Dashboard for Outbound Caller ID completes the configuration.

4.6.4.13. Configuring Open Numbering Plan

When Open Numbering Plan is enabled (see UNIVERGE 3C System Install & Management Manuals), users, addresses and stations are divided over several zones.
Each user, its related addresses and stations shall be assigned to the same zone.
For one or more BCT's operating on their own zone, for each zone a separate CtiUser shall be configured having zone rights on that specific zone. E.g. as shown in the next table:

	BCT-A	BCT-B	BCT-C
Zone: Company-A	Ctiuser-A with zone rights on Company-A		
Zone: Company-B		Ctiuser-B with zone rights on Company-B	
Zone: Company-C			Ctiuser-C with zone rights on Company-C

4.6.5. Business ConneCT installation and configuration

Active Directory
Sphericall
BusinessConnecT

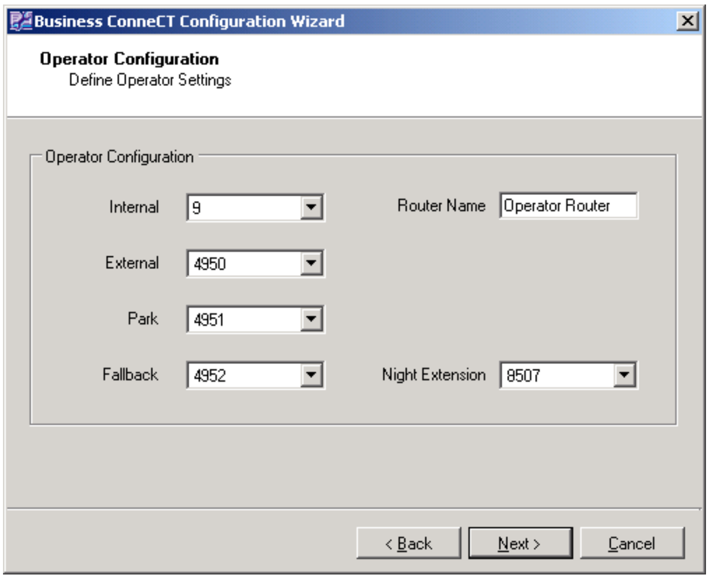
See chapter 6 SERVER PREREQUISITES INSTALLATION for installation of prerequisites and chapter 6.1 Database Installation for installation of the database.

See chapter 7 BCT SERVER PRODUCT INSTALLATION for installation of the BCT Server.

See chapter 8.1.1 Using the Configuration Wizard for the configuration of BCT.
The following notes apply:

1. *PBX Configuration* window:
   PBX Name: Enter a descriptive name for the UNIVERGE 3C Server
   PBX Type: UNIVERGE 3C
   IP Address/Host Name: Enter the IP Address or Host Name of the UNIVERGE 3C Server
   Webservice Port: 443
   PBX Requires Authentic.: Must be checked!
2. *User Authentication* Window:
   Domain Name (AD): Enter the Domain from Active Directory
   User Name: Enter 'CTIuser' (created in 4.6.2.1 How to create a CTIuser account)
   Password: Enter the password for CTIuser
3. *Synchronization with PBX* window:
   If the synchronization fails, make sure that Windows Firewall has been disabled on the BCT and UNIVERGE 3C systems.
4. *License Configuration* window:
   (*For North America*) Select "Licenses in PBX" and click **Next**.
   (*For all other countries*) Select "Licenses in PBX" and click **Next**.
5. *Media Settings* window:
   PBX VoIP Server IP Address: Enter the IP address of the UNIVERGE 3C.
   SIP Authentication Password: This is not used in a UNIVERGE 3C environment, leave blank.
   Secured Connection (TLS/sRTP) Check this when you want the SIP connection and media to be secured so it cannot be monitored.
   TLS is used for connection and sRTP is used for the media.
   Also see 8.1.6.8 Media (via Supervisor)

6. *Operator Configuration* window:
   In our example:



Business ConneCT Configuration Wizard

Operator Configuration
Define Operator Settings

Operator Configuration

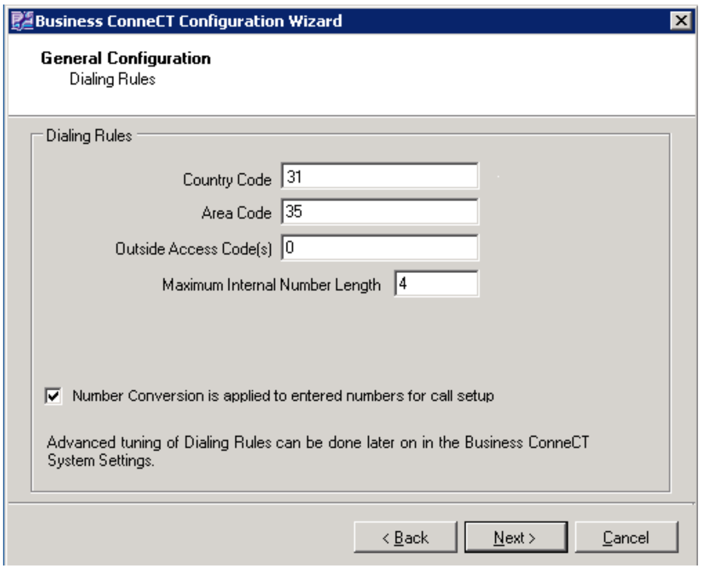
Internal	9	Router Name	Operator Router
External	4950		
Park	4951		
Fallback	4952	Night Extension	8507

7. *Agent Routing Configuration-window:*
   In our example:

Agent Routing Access DNR	4040 (Pilot of Contact Center)
Agent Routing Exception DNR:	8507 (Night Extension)
Agent Logon DNR:	4043 (For phone based agents)
Prompt Recording DNR:	4044
Assign Routing Point:	The Station that the above Extensions are attached.

8. *Dialing Rules* window:

Country Code:	Set to '1' for U.S.A.
Area Code:	Fill in the three-digit Area Code used where BCT is installed.
Outside access code(s):	The first code is used by BCT used for outside access.



Business ConneCT Configuration Wizard

General Configuration
Dialing Rules

Dialing Rules

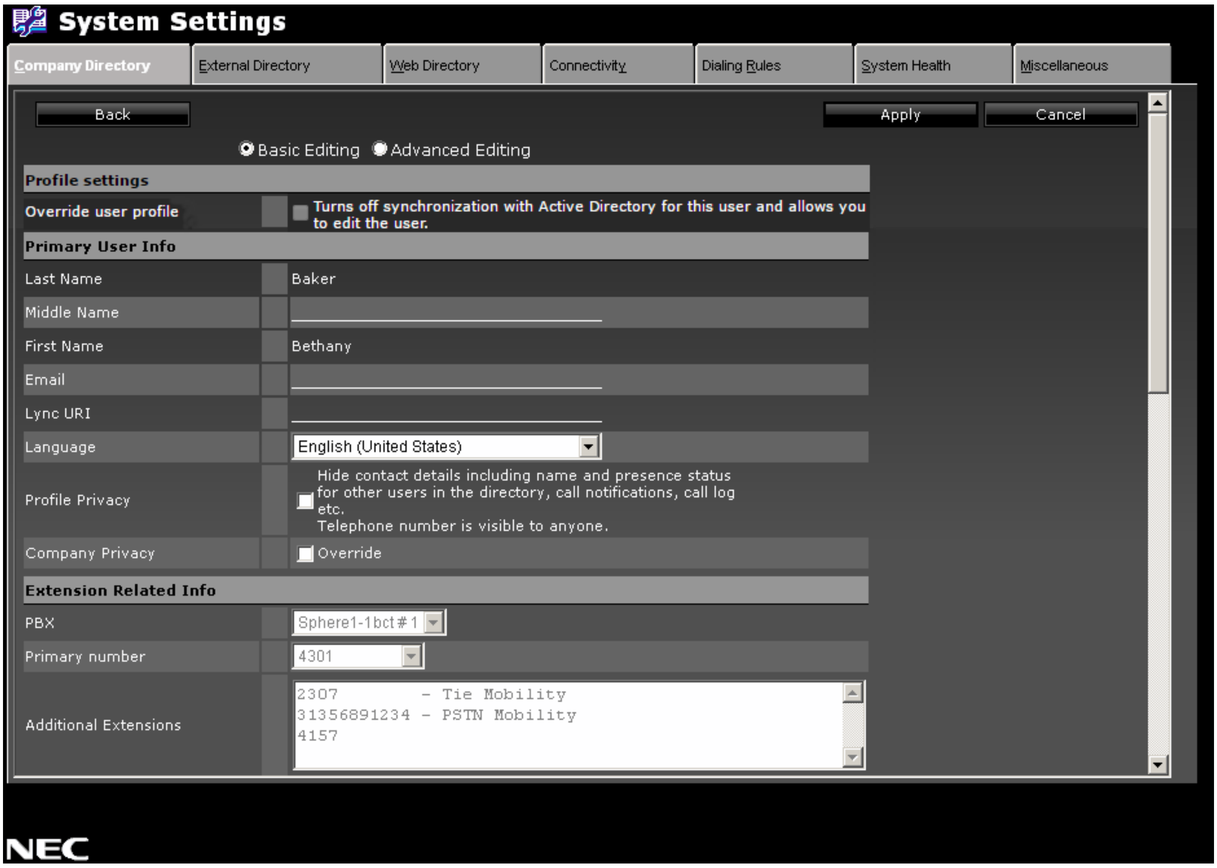
Country Code	31
Area Code	35
Outside Access Code(s)	0
Maximum Internal Number Length	4

☑ Number Conversion is applied to entered numbers for call setup

Advanced tuning of Dialing Rules can be done later on in the Business ConneCT System Settings.

4.6.5.1. Configure users

Select in Edit PBX (Connectivity tab) Zone(s) for a zone selection of users in the company directory. See 8.5.5 Company Directory (User) configuration and 8.5.10 Manually create a BCT user for configuration of users.



● Basic Editing ○ Advanced Editing

Profile settings

Override user profile	□ Turns off synchronization with Active Directory for this user and allows you to edit the user.

Primary User Info

Last Name	Baker
Middle Name	
First Name	Bethany
Email	
Lync URI	
Language	English (United States)
Profile Privacy	□ Hide contact details including name and presence status for other users in the directory, call notifications, call log etc. Telephone number is visible to anyone.
Company Privacy	□ Override

Extension Related Info

PBX	Sphere1-1bct#1
Primary number	4301
Additional Extensions	2307 - Tie Mobility 31356891234 - PSTN Mobility 4157

Figure 4-4-47 Company Directory - Edit 3C User

The following notes apply to the System Settings **User edit** screen:

***Note**: most fields are read-only, as they are imported from 3C and cannot be edited by default in BCT.*

1. Profile Settings section
   This section is not visible by default, unless "User Modification" is checked in the PBX Configuration page.
   If the "Override user profile" checkbox is visible but disabled, the user is "User Centric"and fields are read only.
   For Address Centric user, the "Override user profile" can be checked and allow fields to be mofified.
2. Primary User Info section
   The user may be "User Centric", which implies that more than 1 extension may be assigned to the user. The additional extension will then be visible in a separate field (read-only). The Additional Extensions field may also include the mobility addresses for the user (if available): numbers on another PBX and numbers on the PSTN.

3. Roles section:

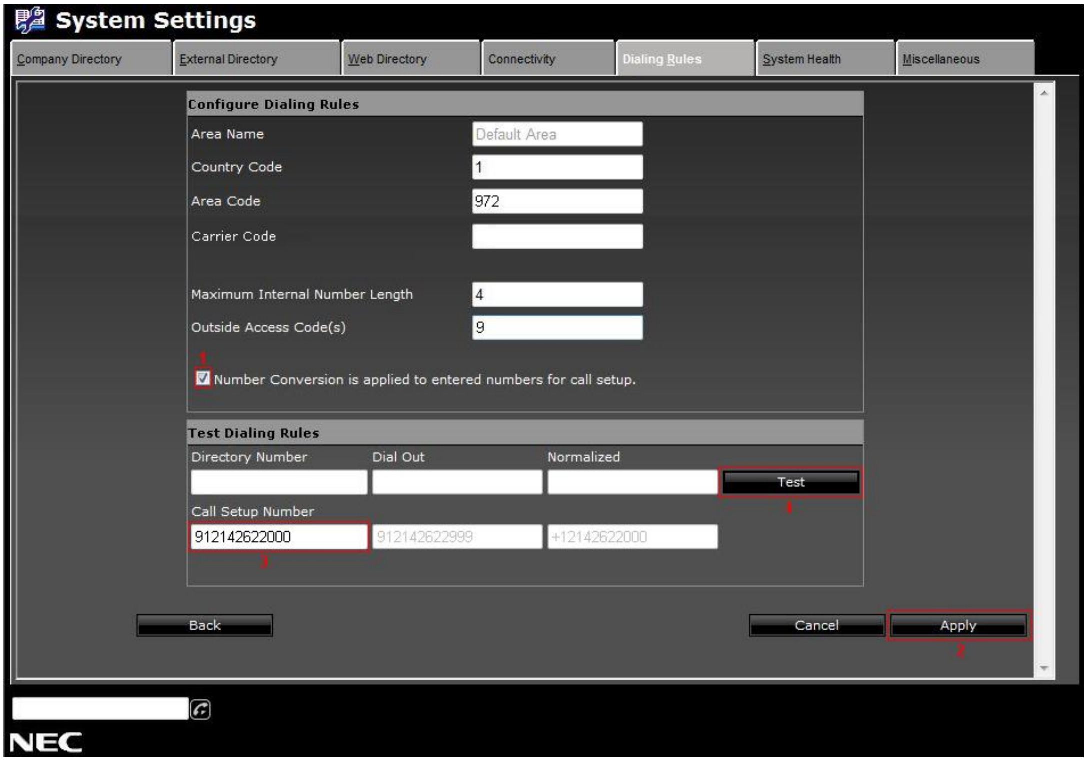
Employee:	Not used with UNIVERGE 3C
Voicemail:	Not used with UNIVERGE 3C (BCT voicemail, doesn't affect UNIVERGE 3C Voicemail)
Operator:	Check if the user will be a BCT Operator
Agent:	Check if the user will be a Contact Center Agent (using BCT desktop client)
Phone Based Agent:	This is checked by default if "Agent" is checked. It can be checked without "Agent" if the user will not use the BCT desktop client.

4.6.5.2. Edit Dialing Rules

See 8.1.11 Dialing Rules for configuration of Dialing Rules.

The following notes apply to the **Configure Dialing Rules** screen:

1. It is necessary to make a modification to the Dialing Rules so that long distance calls will complete.
2. Uncheck "Number Conversion is applied to entered numbers for call setup" and click **Apply**.
3. Test the dialing rule by entering a number "Call Setup Number" and click **Test**.



Configure Dialing Rules

Area Name: Default Area
Country Code: 1
Area Code: 972
Carrier Code:
Maximum Internal Number Length: 4
Outside Access Code(s): 9

☑ Number Conversion is applied to entered numbers for call setup.

Test Dialing Rules

Directory Number	Dial Out	Normalized

Call Setup Number

912142622000	912142622999	+12142622000

4.6.5.3. Suppress Univerge-3C supervision notification

In a Univerge 3C configuration, (3C) users may be allowed to supervise calls of other users. Two types of supervision can be distinguished:

- Monitoring - The supervising party wants to listen to a conversation at the supervised party.
- Barge - The supervising party wants to listen to and talk (take part) in a conversation at the supervised party. This type of supervision is also available from a BCT operator making a call to a busy destination.

Note that this can have legal implications, as in some countries it is not allowed to monitor silently.

4.6.6. Configuration for redundant 3C system

When a 3C system consists of a primary server and one or more secondary servers, BCT is usually connected to the primary server. BCT supports failover to another 3C server when the (connection to the) primary server fails. When the primary server becomes available again it is possible to switch back to the primary server.

Alarms are generated during automatic failover or when a failover fails.   Other significant events are logged as system status events, see 11.2.1.2 System Status.

To configure a redundant 3C system in BCT, see 8.6 Configuring redundant PBX configurations.

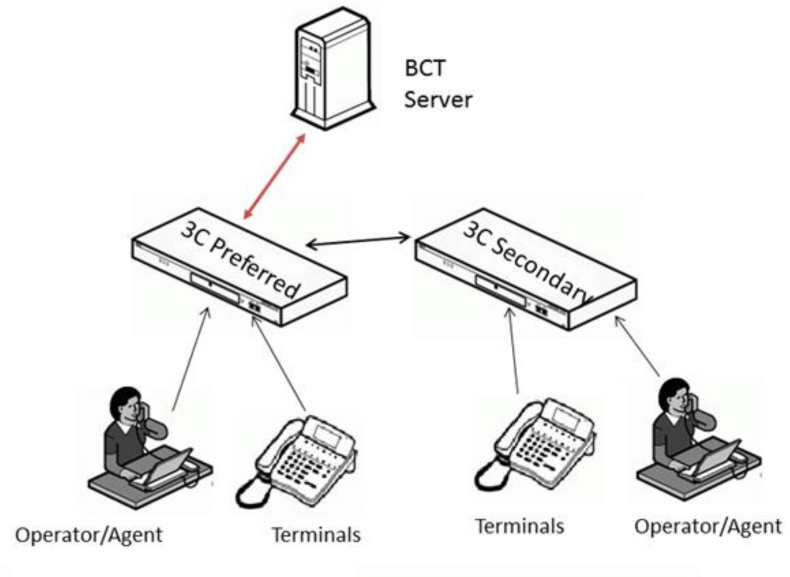


Figure 4-48 Redundant 3C System overview

5. HARDWARE INSTALLATION

5.1. Wallboards (optional)

Wallboards are used to display statistical contact center information. The wallboards are intended to be positioned where agents can see them. BCT supports various types of wallboards; 2 dedicated hardware-based led-matrix wallboard types and one generic software-based wallboard solution.

The two types of supported hardware wallboards are: MessageMaker wallboards and DataDisplay wallboards. The MessageMaker wallboard can also be connected via an IP connection.

5.1.1. MessageMaker wallboard

The MessageMaker wallboard can be connected to a computer via a COM port or via a Local Area Network. The BCT Server and Wallboard must have an IP address from the same subnet.

There are 4 types available:

- MessageMaker 2 line 16 character wallboard. (Part Number: A15911 UD1).
- MessageMaker 2 line 21 character wallboard. (Part Number: A15916 UD1).
- MessageMaker 4 line 16 character wallboard. (Part Number: A15917 UD1).
- MessageMaker 4 line 21 character wallboard. (Part Number: A15918 UD1).

The MessageMaker wallboard must be ordered directly from the manufacturer (www.messagemaker.co.uk).

5.1.1.1. MessageMaker wallboard installation via COM port

Figure 5-1 Wallboard configuration shows how a MessageMaker wallboard must be connected to the computer that contains the wallboard drivers. The DIP switches are covered by a small metal plate.

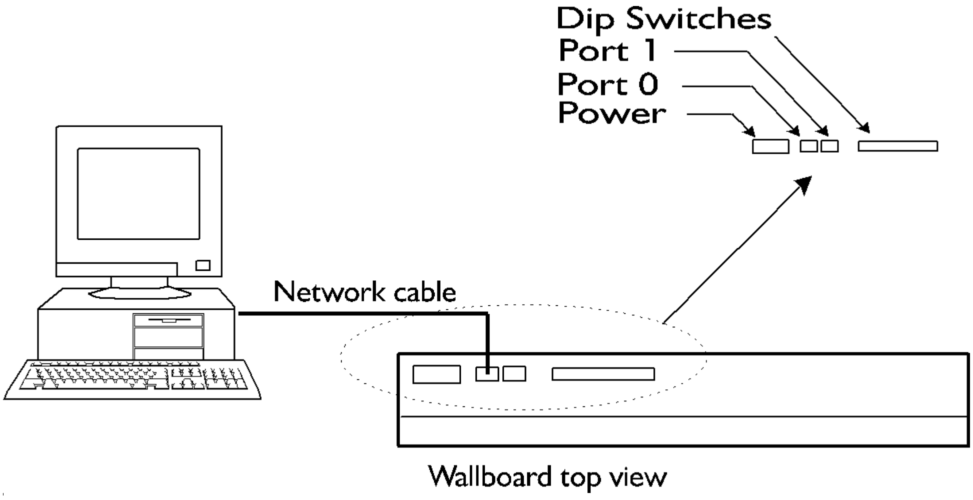


Figure 5-1 Wallboard configuration

1. Connect the “9 pin D to RJ45 adapter” to a free COM port.

2. Make a connection between the “9 pin D to RJ45 adapter” and port 0 of the wallboard. For this connection you need a straight network cable with RJ45 connectors, this cable is not included in the Wallboard package.

3. Select address 1.

4. Remove the small metal plate that covers the DIP Switches.

5. Set switch 1 on and switch, 2, 3, 4, 5, 6, 7 and 8 off. Address 1 is now selected. When you plug in the power, the wallboard will start a self-test. During this test the selected address will be displayed (shortly!).

At this moment the hardware configuration is ready. Continue with the software configuration. For creating and configuring wallboards, refer to the BCT Administrator Guide and BCT Supervisor Guide.

5.1.1.2. MessageMaker wallboard installation via LAN

The MessageMaker wallboard can also be connected and controlled via a Local Area Network. The network connector is located on the right side of the wallboard.

Connect the wallboard to the network. Near the network connector you can also find the DIP switches. The functions of these switches are described in Table 5-1 DIP Switches for IP connection.

Switch	Explanation	
1	Always off	
2	Always off	
3	Always off	
4	Always off	
5	Always off	
6	On for default IP address and port number	Off to use the IP address and port number from EPROM
7	On for updating EPROM with new values	Off to protect EPROM
8	On for normal operation	Off to select IP communications mode

Table 5-1 DIP Switches for IP connection

Execute the following steps to configure the IP address on the wallboard:

1. Set the DIP switches to set-up mode. The DIP switches are located near the network connector.

Note: *These are not the DIP switches that are used for the serial port address selection.*

Set switch 1, 2, 3, 4, and 5 to off.

2. Set switch 6 to on. By switching this switch to on, the wallboard will start with the default IP address and port number.

IP address = 192.168.3.200

Port = 3500

3. Switch 7 must be set to on, this allows the bootprom to be updated with new values.

4. Switch 8 must be set to off to select the IP configuration mode.

5. Power up the wallboard

6. **Change the IP address** (of the computer on which you install the MessageMaker IP configuration tool)

The wallboard is only reachable with a computer that has an IP address from the same subnet, therefore you must change the IP address on the computer that is connected to the wallboard (you can also use another computer to setup the wallboard).

Change the IP address to an address from the 192.168.3.0 subnet.
Do not use 192.168.3.200, this address is used by the wallboard.

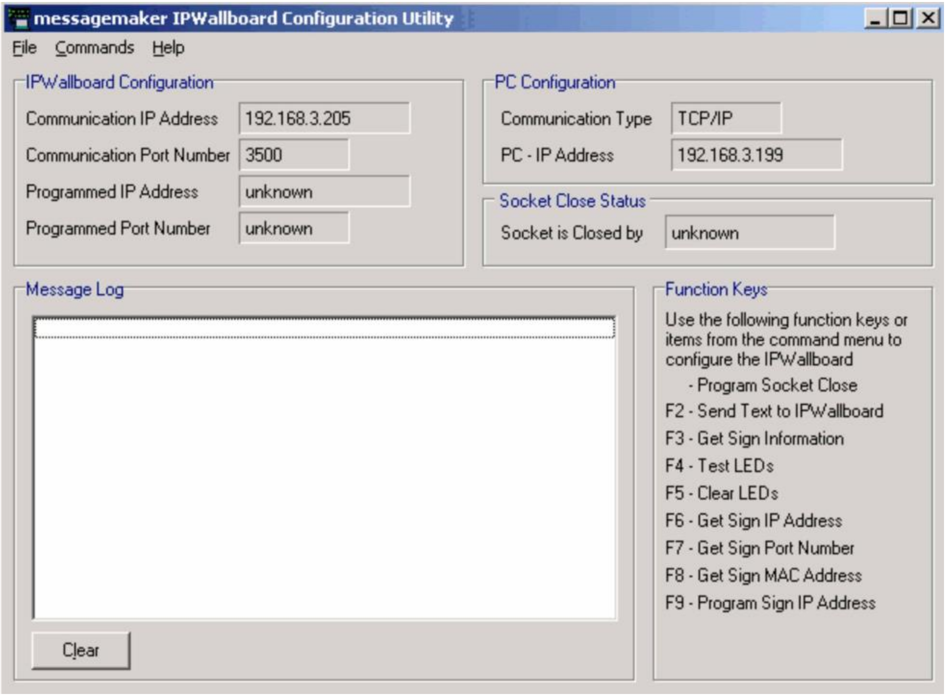
7. Reboot the computer. After this you should be able to ping the wallboard. When the ping request is successful, you can continue with the next step.

8. Install MessageMaker IP configuration tool

At the end of the installation, you will be asked if you would like to launch the program, select **Yes** and click **Finish**.

The next time you need to use the IP configuration program, select **Start > Programs > ConfigIPW > ConfigIPW**.

The following window will appear:



IPWallboard Configuration

Communication IP Address: 192.168.3.205
Communication Port Number: 3500
Programmed IP Address: unknown
Programmed Port Number: unknown

PC Configuration

Communication Type: TCP/IP
PC - IP Address: 192.168.3.199

Socket Close Status

Socket is Closed by: unknown

Message Log

Function Keys

Use the following function keys or items from the command menu to configure the IPWallboard

- Program Socket Close
F2 - Send Text to IPWallboard
F3 - Get Sign Information
F4 - Test LEDs
F5 - Clear LEDs
F6 - Get Sign IP Address
F7 - Get Sign Port Number
F8 - Get Sign MAC Address
F9 - Program Sign IP Address

Figure 5-2 IP config main window

The software is now installed.

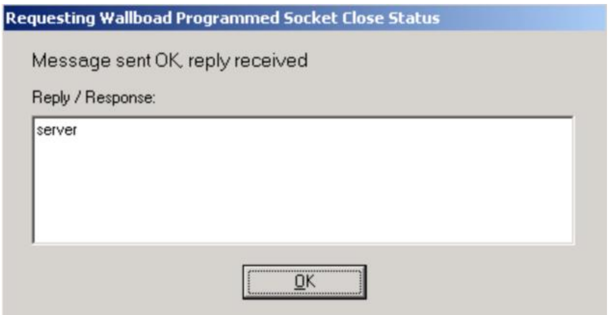
9. Set up the wallboard connection

As you can see in Figure 5-2 IP config main window, there are two IP addresses. The right one is the IP address from your computer and the left one is the IP address that is used to connect to the wallboard. This address is not correct and needs to be changed to the default one (192.168.3.200).

Select **Setup** from the **File** menu. Enter the value “192.168.3.200” and click **OK**.

At this moment you should be able to communicate with the wallboard.

Select **Program Socket Close** from the **Commands** menu. The result should be as shown in Figure 5-3 Wallboard message window Click **OK** to continue.



Requesting Wallboad Programmed Socket Close Status

Message sent OK, reply received

Reply / Response:

server

Figure 5-3 Wallboard message window

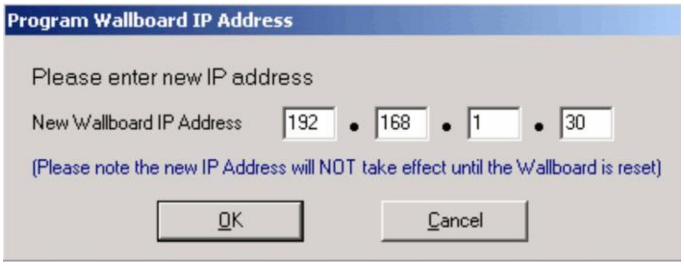
The computer is now able to communicate with the wallboard. At this moment you can perform a LED test, (select F4) or send some information to the wallboard (F2). All actions are listed in the Message Log window. Continue with the next step.

10. Entering the correct IP address

At this moment the wallboard uses the fixed default IP address and port number. Check if the port number 3500 is used on your computer. (c:\Windows\Sytem32\drivers\etc\services). If the number is not used, there is no need to change the port number.

The wallboard contains an EPROM that can be programmed with an IP address. So by entering a new IP address you are not changing the default one. Also when an IP address is entered in the EPROM, it is still possible to use the fixed default one.

Select **Program SignIP Address** from the **Commands** menu or press F9. The following window appears:



Program Wallboard IP Address

Please enter new IP address

New Wallboard IP Address 192 . 168 . 1 . 30

(Please note the new IP Address will NOT take effect until the Wallboard is reset)

Figure 5-4 New IP address window

Enter the correct IP address.

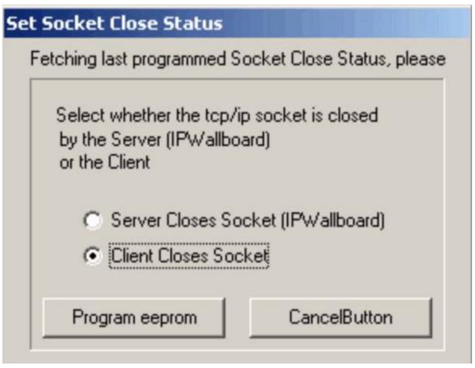
The system will return an output window that should display “ProgIP OK". If the system returns with the message “PRog error”, the action failed. Most likely because DIP switch 7 is set to “off”. In this switch is set to off the EPROM is in the protected mode. You can check that the new IP address is entered correctly by selecting F6. The New IP address will only be used after a power down of the wallboard and correct DIP switch settings.

11. Set the correct socket close option

The wallboard uses a socket to communicate with the BCT Supervisor Dashboard. This socket must be controlled by the BCT Supervisor Dashboard (Client).

Select “Program Socket Close” from the “Function Keys” area, as shown in Figure 5-2 IP config main window

Mark “Client Close Socket”, as shown in Figure 5-5 Set Socket Close Status window



Set Socket Close Status

Fetching last programmed Socket Close Status, please

Select whether the tcp/ip socket is closed
by the Server (IPWallboard)
or the Client

○ Server Closes Socket (IPWallboard)

● Client Closes Socket

Figure 5-5 Set Socket Close Status window

Select “Program eeprom” to store the correct close option in the eeprom.

12. Set the DIP switches to the normal operation mode

Power down the wallboard.
Set DIP switch 6 to off and switch 7 to off.
Power up the wallboard.

The wallboard performs a self-test. During the self-test the new IP address is displayed on the last line of the wallboard (shortly!).

Change the IP address of the computer to an IP address that belongs to the subnet of the entered IP address.

13. Test the wallboard with the new IP address

14. Start the ConfigIPW program.

The Communication IP Address must be changed to the new entered IP address. Select **Setup** from the **File** menu.

Enter the IP address that you entered in step 5 and click **OK**.

Select **Program Socket Close** from the **Commands** menu. The result should be as shown in Figure 5-3 Wallboard message window. Click **OK** to continue.

Send some information to the wallboard (F2). Check the result.

If more than one wallboard is used, repeat the above described actions for all wallboards.

At this moment the wallboard is correctly configured for network use. For creating and configuring wallboards, refer to the BCT Administrator Guide and BCT Supervisor Guide.

5.1.1.3. Other features of the MessageMaker wallboard

DIL switches 5 and 6 are used to set the data speed of the wallboard. This should be set to 1200 Baud (which is the default).

DIL SWITCH NUMBER		**BAUD RATE**
5	**6**	
On	On	9600
Off	On	4800
On	Off	2400
Off	Off	1200 - default

Table 5-2 DIL Switches Data Speed settings

DIL switches 7 and 8 are used to select a test mode.

DIL SWITCH NUMBER		**TEST MODE**
7	**8**	
On	On	Normal Mode - default
Off	On	Stripe test
On	Off	Full screen
Off	Off	Information screen

Table 5-3 DIL Switches Test Mode

- Normal mode. After testing the wallboard, set the switches to this setting for normal operation.

- Stripe test. This setting generates a stream of moving stripes after power up. This is used to test if the power supply and the display driver circuits are working correctly.

- Full screen. This setting puts all LEDs on simultaneously after power up.
WARNING: DO NOT USE THIS MODE FOR MORE THAN 30 SECONDS.

- Information Screen. This setting is used to show the following product data after power up:

  V: The EPROM version number (100 means version 1.00).

L: The Logic board version number.

N: The Network number (address switch setting).

B: The Baud rate setting (12 means 1200, 24 means 2400 etc.).

5.1.2. DataDisplay wallboard

The DataDisplay wallboard is connected to the BCT computer with a COM port connection. There are two types available: a 10 character wallboard and a 20 character wallboard.

5.1.2.1. DataDisplay wallboard cabling

Before installing the wallboard it is recommended to measure the distance between the required wallboard positions and the computer.

DO NOT connect wallboards in a star configuration, i.e. all wallboards with a separate cable to the computer.

The following diagrams show how to connect wallboards in series or in parallel.

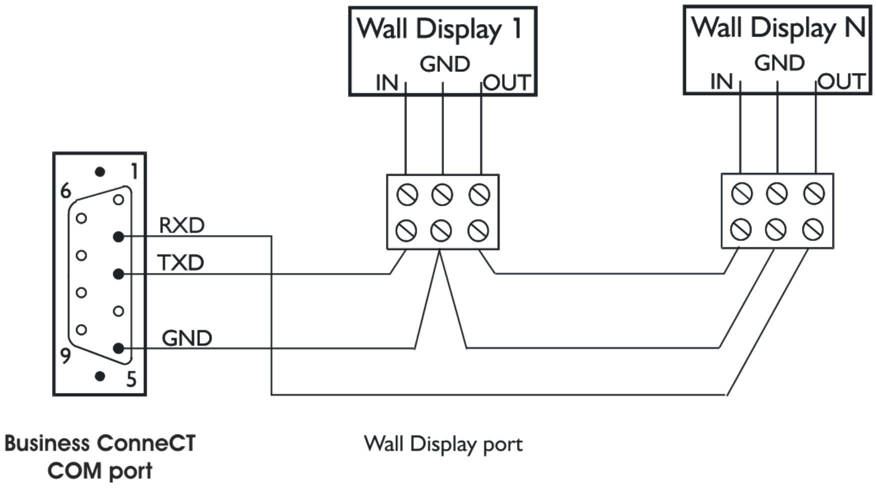


Figure 5-6 Connecting wallboards in series

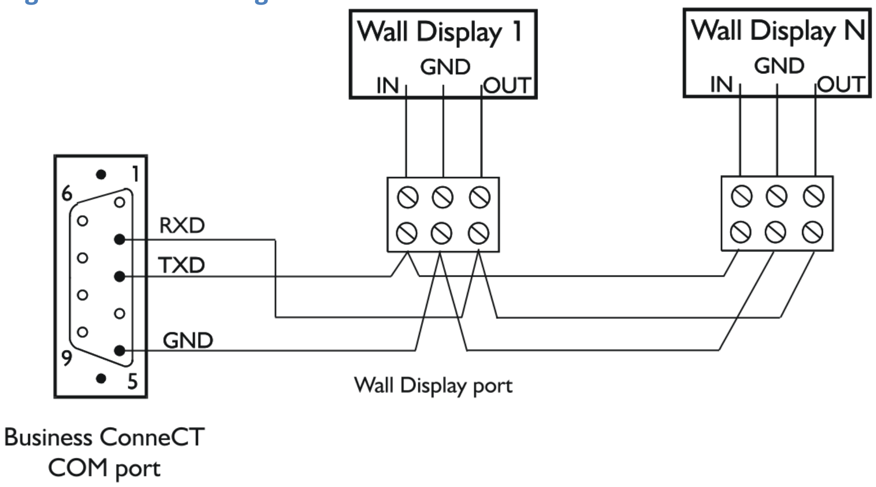


Figure 5-7 Connecting wallboards in parallel

5.1.2.2. DataDisplay wallboard hardware overview and installation

The wallboard is delivered with the following items:

- Wallboard.
- Network module (also known as address switch).
- Power supply unit (transformer).
- Cable.
- Connector box Faddist.
- Assembly set (brackets, screws, wall plugs).

How to install the DataDisplay wallboard

Ensure that the wallboards are disconnected from the mains during the installation.

1. Mount the wallboards in the required positions. It may be necessary to also mount the transformer in a suitable position.

If you only have 1 wallboard then this can be installed without the use of connector boxes, go to step 4.

If you have more wallboards then you need to install connector boxes. See Figure 5-8 Example of Faddist Box Connection.

Cut the cable to a suitable length, retaining the 3,5 mm three conductor mini jack (this mini jack must be plugged into the wallboard when it is installed). Connect the cable to the connector block in the **Faddist** box(es).

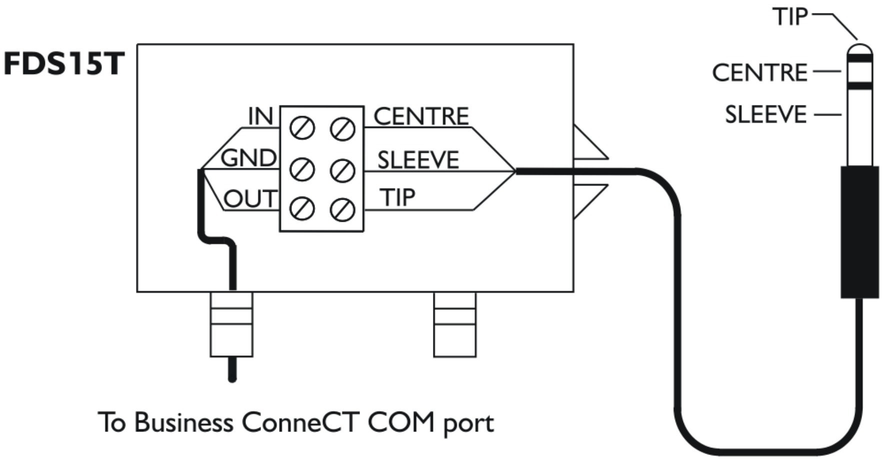


Figure 5-8 Example of Faddist Box Connection

2. Link the connector boxes together, see Figure 5-8 Example of Faddist Box Connection

   - If you have 1 wallboard, connect it directly to the BCT computer.
     If you have more than 1 wallboard, connect the first connector box to the BCT computer.

   - The wallboards were delivered with *address switches*. More recently this has been replaced by a *dipswitch*.

     With Address switches
     Set the address switches of the 'Network Module' on the wallboards to a value 01...09 (see Figure 5-9 Address Settings on wallboard). The first wallboard uses address 01. Ensure that the Network Module is fitted centrally in its socket.

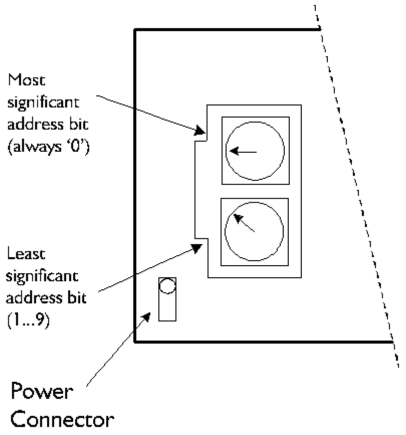

Most significant address bit (always '0')
Least significant address bit (1...9)
Power Connector

Figure 5-9 Address Settings on wallboard

With dipswitch

You can set the dipswitches as follows:

Dipswitch			Address
3	2	1	
Off	Off	On	21
Off	On	Off	22
Off	On	On	23
On	Off	Off	24
On	Off	On	25
On	On	Off	26

3. Connect the transformer of each wallboard in turn and plug it in to the mains supply. The wallboard gives a confirmation beep and a message may be shown. The message can be the message sent by BCT or the manufacturers test message or the last message that has been sent to the wallboard.

5.1.3. Software wallboard

The BCT software-based wallboard solution only requires a standard windows PC with a monitor attached to it and Microsoft PowerPoint installed. For a complete description on the required installation steps please refer to Soft Wallboard.

6. SERVER PREREQUISITES INSTALLATION

This chapter describes how to install the BCT Server prerequisites software. The software is stored on one DVD. When starting BCT Server installation via **BCT DVD Main Menu** all the required prerequisites software is checked and when missing it will be installed automatically.

This includes e.g. Microsoft Visual C++ Runtime and Microsoft .NET Framework.

WARNING: *BCT cannot be installed on a PC which is configured as a Domain Controller.*

For the prerequisite check related to SQL server only a check is done and a warning is given if no local SQL server is detected. This is done because also a remote SQL server can be used. See next chapter for additional information regarding setup of the SQL Server functionality.

6.1. Database Installation

If a customer already has a SQL Server deployed, you can consider using this SQL Server for BCT. In that case, you don't need to install the SQL server software. In cases of a high load system, install the SQL server software on another PC than the BCT server.

Non-English SQL Server versions are supported. When BCT is installed, it automatically uses the language of the SQL database. You cannot change the SQL Server Language after BCT has been installed.

BCT supports secure connections to remote SQL server using TLS 1.2 protocol (even on servers with TLS 1.0 and 1.1 protocols disabled). Please refer to "TLS 1.2 support for Microsoft SQL Server" for additional information, e.g. how to determine whether your current version of SQL Server already has support for TLS 1.2.

Note*: Secure connections from BCT to remote SQL server using TLS 1.2 protocol are not supported when BCT is running on Windows Server 2008 R2 or Windows 7.*

Note*: The BCT database installation selects "Simple Recovery" as default recovery model for the SQL transaction log.*

"Simple Recovery" means that transactions are removed from the transaction log, when committed. This prevents the transaction log from growing continuously. However, be aware that regular backup is required to prevent possible loss of data.

Installing SQL Server 2016 Express Edition via BCT Installer

Preconditions:

1. Supported for next 64-bit operating system versions of Windows Server 2012 (R2), Windows Server 2016, Windows Server 2019, Windows 8.1 and Windows 10.

2. For Windows Server 2012 R2 it is required to have Windows Update KB2919355 installed.

Steps:

1. Insert the BCT product DVD. The **BCT DVD Main Menu** window appears. If not, double click **D:\Autorun.exe** (where D is the drive letter of your DVD drive).

2. Install the required prerequisites (see 'Preconditions' above)

3. Select 'SQL Server 2016 Express Edition'

4. Select 'Default SQL 2016 Instance' or 'Named SQL 2016 Instance'

5. Enter the password for 'sa' administrator account.

Installing SQL Server Management Studio

Starting from SQL Server 2016 the **SQL Server Management Studio** is a stand-alone install outside of the SQL Server release. This tool is used for maintenance actions (e.g. view content of tables). Starting from BCT 8.10.x this install is not available anymore on the DVD. It is recommended to download the latest version from: https://msdn.microsoft.com/en-us/library/mt238290.aspx
The SQL Server Management Studio is free (no SQL server license required anymore) and is updated on a regular basis.

If using **SQL Server 2016 Express Edition**, note the following:

- For general SQL Server limitations see 'BCT Boundary Specification'.
- SQL Server 2016 Express Edition does not support scheduled backups (SQL agent is not included in this edition). For scheduled backups, we recommend a freeware database backup tool like "SQL Backup and FTP" (www.sqlbackupandftp.com).

Installing SQL Server (Standard or Express Edition) manually

If manually installing SQL Server (Standard or Express Edition) be aware of the following:

- SQL Server – Service(s) must be configured to run under Local System Account.
- Select 'SQL Server and Windows Authentication Mode' (also known as mixed mode).
- Enable the protocols 'TCP/IP' and 'Named Pipes' for the server.

7. BCT SERVER PRODUCT INSTALLATION

This section describes how to install the BCT server software. Installation of the BCT desktop client and the BCT Contact Center Client software is described in 9 CLIENT INSTALLATION AND CONFIGURATION.

Preconditions:

1. For the BCT server ensure the power options are configured in such a way that the PC never goes into standby mode.

2. Make sure the PBX has the required software version. (The Release Notes for BCT specifies the required version.)

3. Check the system requirements for BCT Server.

4. Check the IP address and subnet mask of the PBX. The address must be reachable from your BCT Server. Ping the IP address from your BCT server.

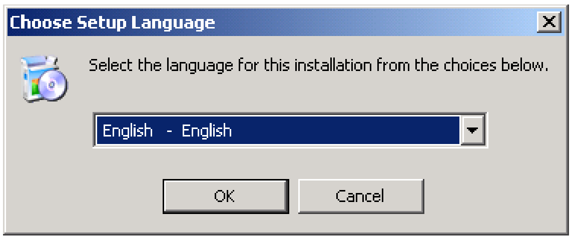
5. Enable the Windows Firewall.

6. In case BCT is connected to UNIVERGE 3C : add the server to the domain of which the UNIVERGE 3C server is a member server as well

Steps:

1. Insert the BCT product DVD. The **BCT DVD Main Menu** window appears. If not, double click D:\autorun.exe (where D is the drive letter of your DVD drive).

2. Select and click “Business ConneCT Server”.
   You are asked first to select a language.



Choose Setup Language

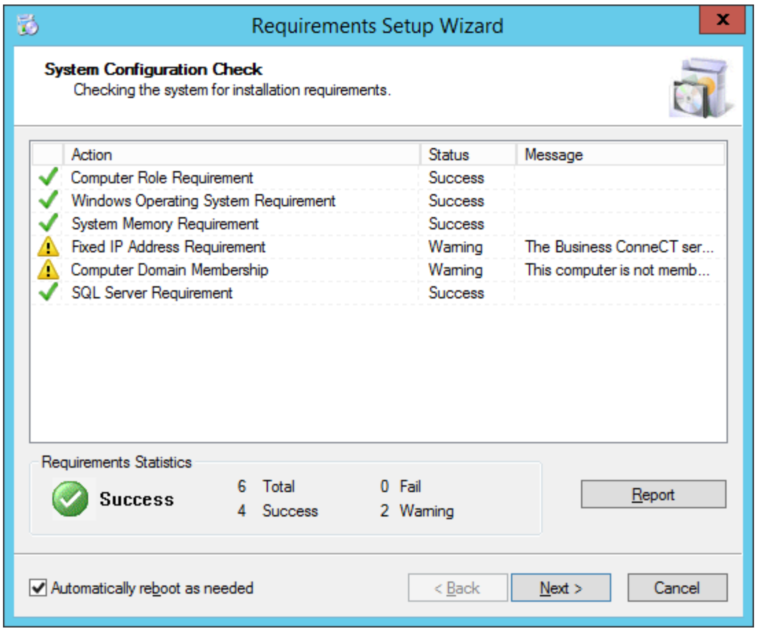
Select the language for this installation from the choices below.

English - English

Figure 7-1 Language Selection window

Select the language and click on **OK**.

The Requirements Setup Wizard checks that the server meets the configuration requirements. Here is an example:



System Configuration Check
Checking the system for installation requirements.

	Action	Status	Message
✓	Computer Role Requirement	Success	
✓	Windows Operating System Requirement	Success	
✓	System Memory Requirement	Success	
⚠	Fixed IP Address Requirement	Warning	The Business ConneCT ser...
⚠	Computer Domain Membership	Warning	This computer is not memb...
✓	SQL Server Requirement	Success	

Requirements Statistics
Success
6 Total
4 Success
0 Fail
2 Warning

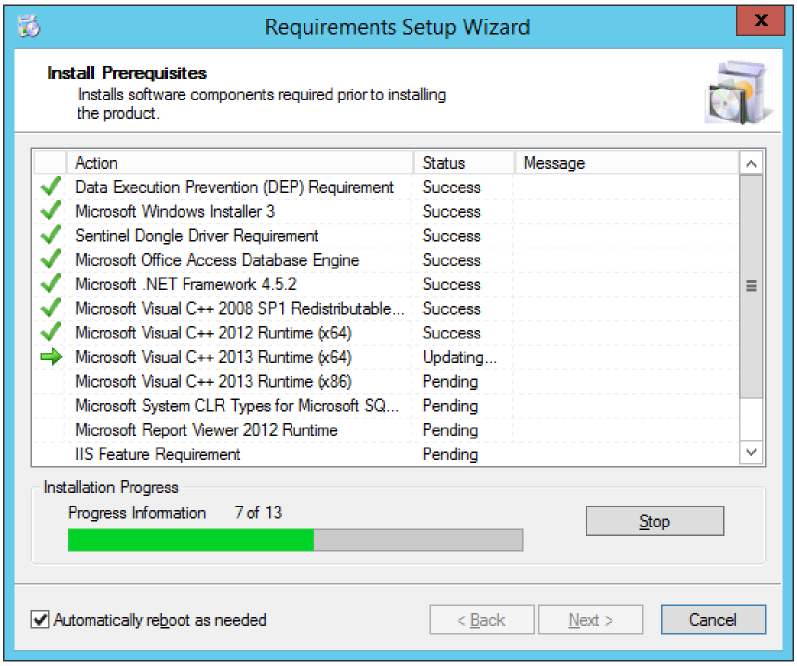
☑ Automatically reboot as needed

Figure 7-2 System Configuration Check Window

3. Install any missing components. You can leave the Wizard open while you do this. To re-check an item, right click on the item and select Re-evaluate.

4. When all items are successful, click **Next**.

The “Install Prerequisites”-window appears. The Wizard checks for required software and installs any missing items.



Install Prerequisites
Installs software components required prior to installing the product.

	Action	Status	Message
✓	Data Execution Prevention (DEP) Requirement	Success	
✓	Microsoft Windows Installer 3	Success	
✓	Sentinel Dongle Driver Requirement	Success	
✓	Microsoft Office Access Database Engine	Success	
✓	Microsoft .NET Framework 4.5.2	Success	
✓	Microsoft Visual C++ 2008 SP1 Redistributable...	Success	
✓	Microsoft Visual C++ 2012 Runtime (x64)	Success	
➡	Microsoft Visual C++ 2013 Runtime (x64)	Updating...	
	Microsoft Visual C++ 2013 Runtime (x86)	Pending	
	Microsoft System CLR Types for Microsoft SQ...	Pending	
	Microsoft Report Viewer 2012 Runtime	Pending	
	IIS Feature Requirement	Pending	

Installation Progress
Progress Information 7 of 13

☑ Automatically reboot as needed

Figure 7-3 Install Prerequisites window

If the Data Execution Prevention requirement is not met, you will get a dialog box where you must select “Turn on DEP for essential Windows programs and services only”.

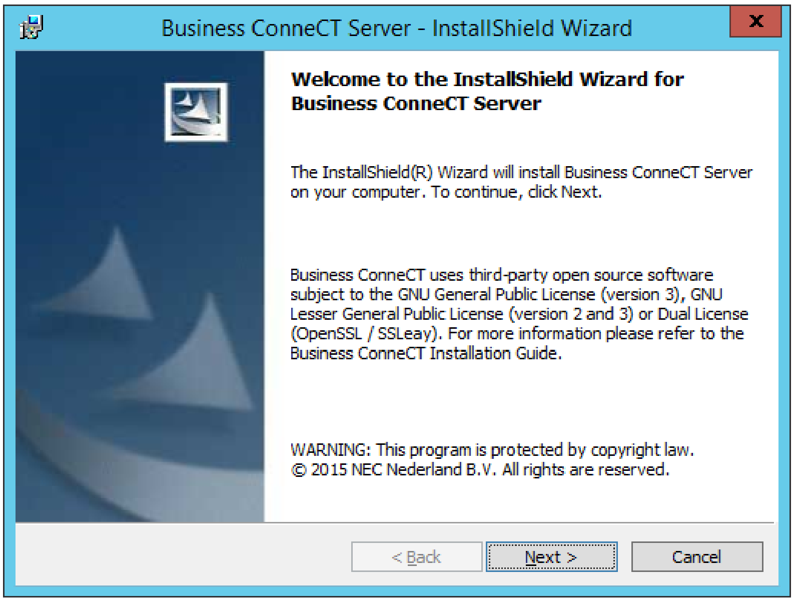
When all items are successful, click **Next**.

If the Security Alert - Driver Installation dialog box appears, click **Yes**.

5. The "Selected Option Information"-window shows the installation progress.
   When finished, click **Next**.
   If the Security Alert - Driver Installation dialog box appears, click **Yes**.

6. When asked to restart the system, click **Restart Now**. Wait until the PC is restarted and the installation continues

7. The "Welcome to the InstallShield Wizard for Business ConneCT Server"-window appears.



Business ConneCT Server - InstallShield Wizard

Welcome to the InstallShield Wizard for Business ConneCT Server

The InstallShield(R) Wizard will install Business ConneCT Server on your computer. To continue, click Next.

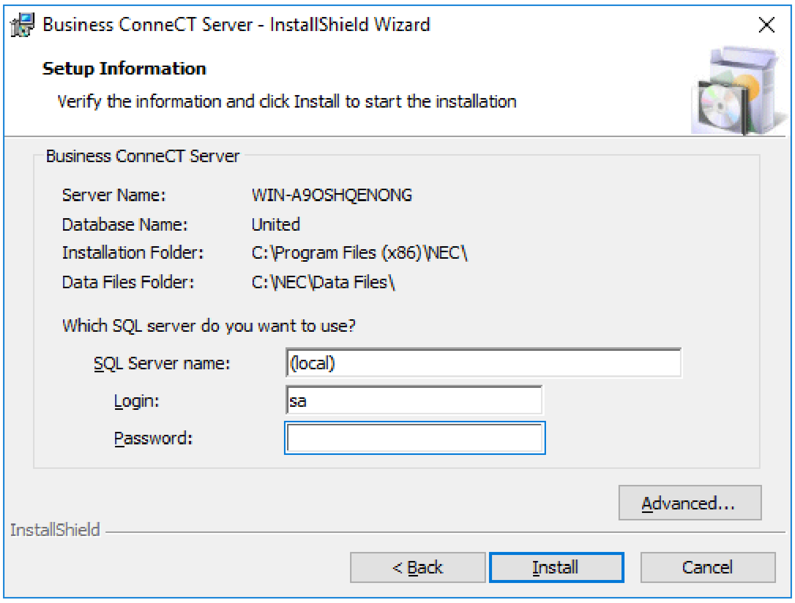
Business ConneCT uses third-party open source software subject to the GNU General Public License (version 3), GNU Lesser General Public License (version 2 and 3) or Dual License (OpenSSL / SSLeay). For more information please refer to the Business ConneCT Installation Guide.

WARNING: This program is protected by copyright law.
© 2015 NEC Nederland B.V. All rights are reserved.

Figure 7-4 InstallShield Welcome window

Click **Next**.

8. The "Setup Information" window appears.



Business ConneCT Server - InstallShield Wizard

Setup Information

Verify the information and click Install to start the installation

Business ConneCT Server

Server Name: WIN-A9OSHQENONG
Database Name: United
Installation Folder: C:\Program Files (x86)\NEC\
Data Files Folder: C:\NEC\Data Files\

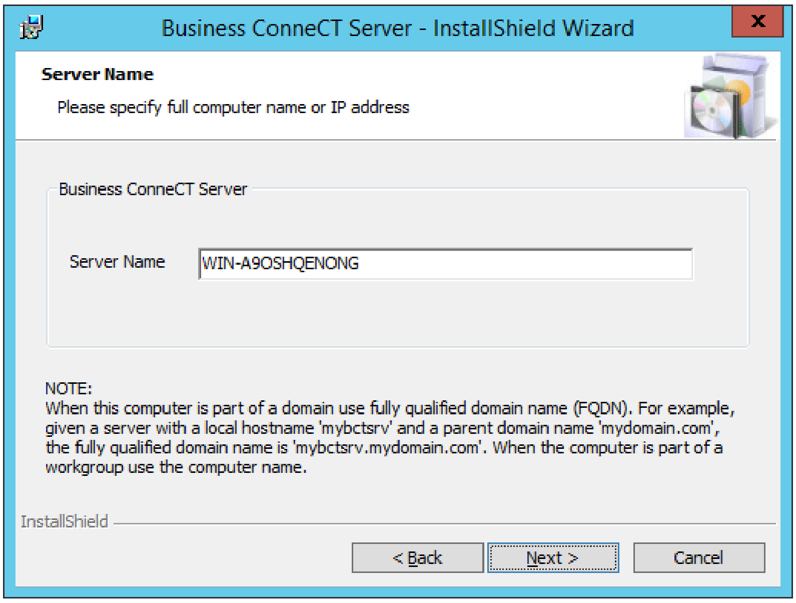
Which SQL server do you want to use?

SQL Server name: (local)
Login: sa
Password:

Figure 7-5 Setup Information Window

Enter the Database location, username sa and password. When all is OK, click **Install**. Continue with step 14 The "Installing" window appears.
If you wish to change the server name, the name of the BCT SQL database or installation folders click Advanced.

9. The "Server name" window appears.



Server Name

Please specify full computer name or IP address

Business ConneCT Server

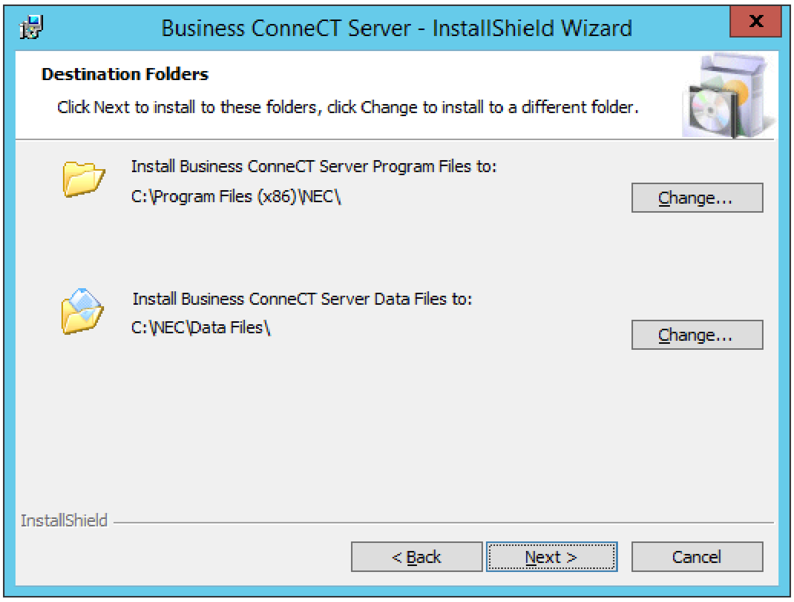
Server Name: WIN-A9OSHQENONG

NOTE:
When this computer is part of a domain use fully qualified domain name (FQDN). For example, given a server with a local hostname 'mybctsrv' and a parent domain name 'mydomain.com', the fully qualified domain name is 'mybctsrv.mydomain.com'. When the computer is part of a workgroup use the computer name.

Figure 7-6 Server Name window

Enter the server name and click **Next**.

10. The "Destination Folders" window appears.



Destination Folders

Click Next to install to these folders, click Change to install to a different folder.

Install Business ConneCT Server Program Files to:
C:\Program Files (x86)\NEC\

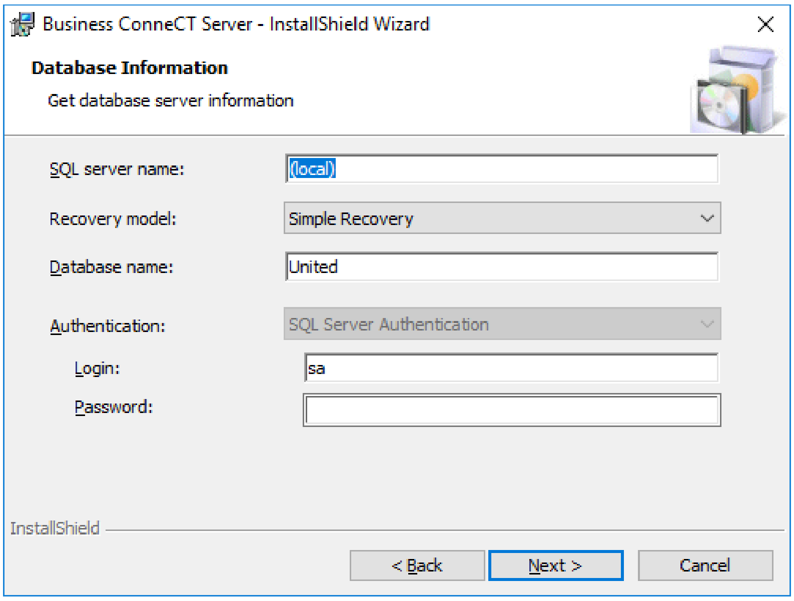
Install Business ConneCT Server Data Files to:
C:\NEC\Data Files\

Figure 7-7 Destination Folders window

Choose the **Destination Folders** and click **Next**.
- Default path for executable files: **C:\Program Files (x86)\NEC\**

- Default path for data files: **C:\NEC\Data Files**
Click **Next.**

11. The "Database Information" window appears.



Business ConneCT Server - InstallShield Wizard

Database Information

Get database server information

SQL server name: (local)

Recovery model: Simple Recovery

Database name: United

Authentication: SQL Server Authentication

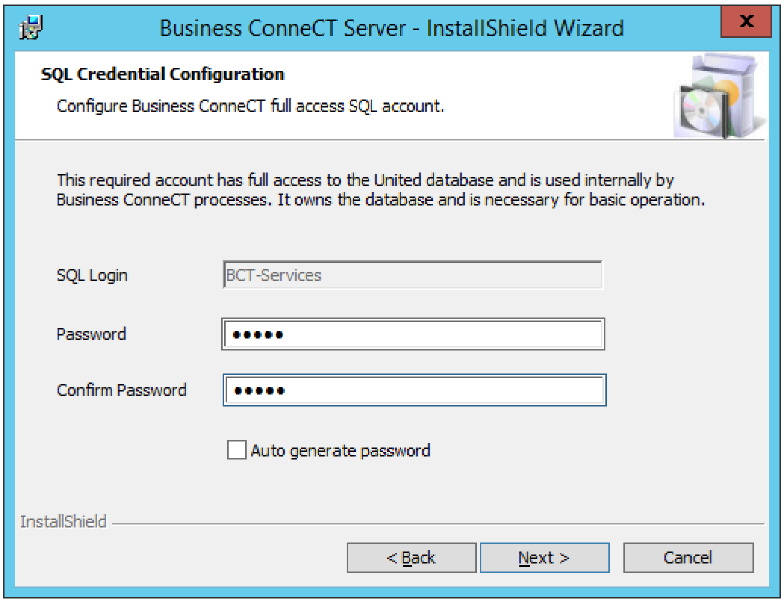
Login: sa

Password:

Figure 7-8 Database Location window

Enter the **Database location**, username **sa** and password.
Optionally change the name of the BCT SQL database and click **Next**.
The “sa” user is only used during installation, for normal BCT operation the SQL login "BCT-Services" is created on the SQL server.

12. The “SQL Credential Configuration” window appears



Business ConneCT Server - InstallShield Wizard

SQL Credential Configuration

Configure Business ConneCT full access SQL account.

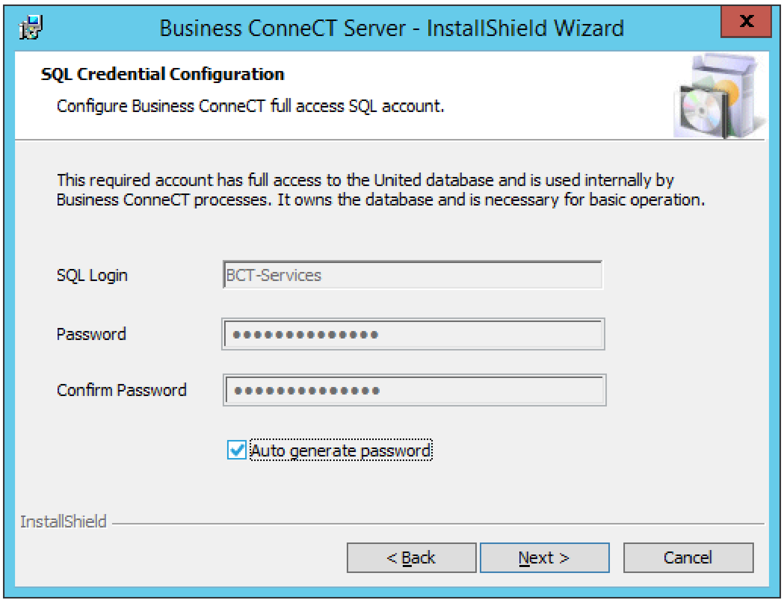
This required account has full access to the United database and is used internally by Business ConneCT processes. It owns the database and is necessary for basic operation.

SQL Login: BCT-Services

Password: •••••

Confirm Password: •••••

□ Auto generate password



Business ConneCT Server - InstallShield Wizard

SQL Credential Configuration

Configure Business ConneCT full access SQL account.

This required account has full access to the United database and is used internally by Business ConneCT processes. It owns the database and is necessary for basic operation.

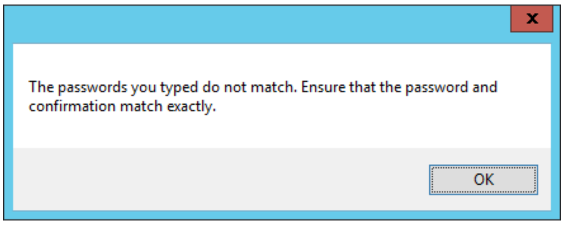
SQL Login: BCT-Services

Password: ••••••••••••••

Confirm Password: ••••••••••••••

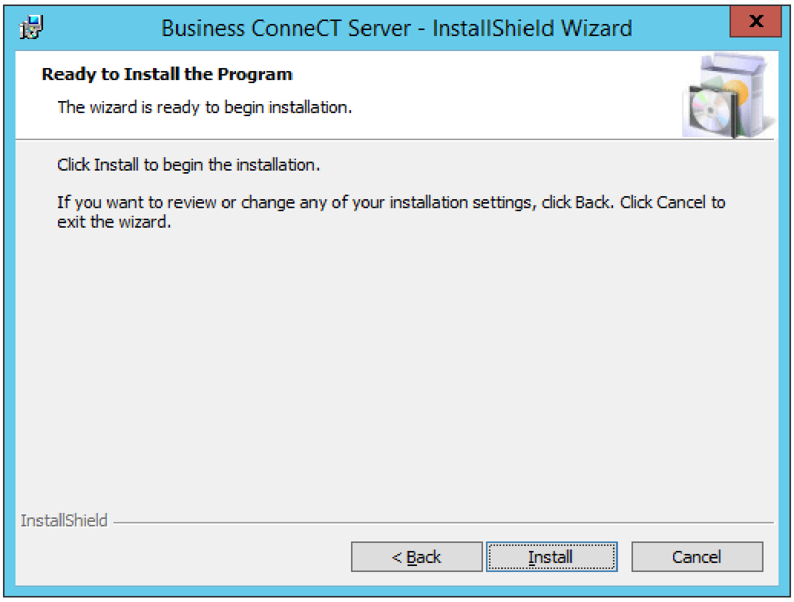
☑ Auto generate password

Enter either a manual password (inclusive confirmation) or select checkbox to automatically generate a password for the BCT SQL account and click **Next**. When password and confirmed password does not match next message is shown.



The passwords you typed do not match. Ensure that the password and confirmation match exactly.

13. The “Ready to Install”-window appears.



Business ConneCT Server - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

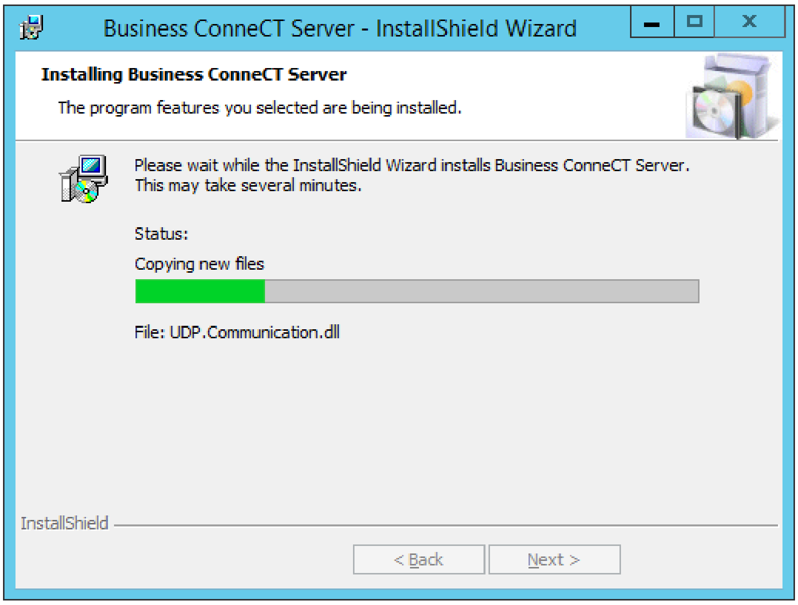
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 7-9 Ready to Install window

You can go back to the previous steps if required.
When all is OK, click **Install**.

14. The "Installing" window appears.


Business ConneCT Server - InstallShield Wizard

Installing Business ConneCT Server

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Business ConneCT Server. This may take several minutes.

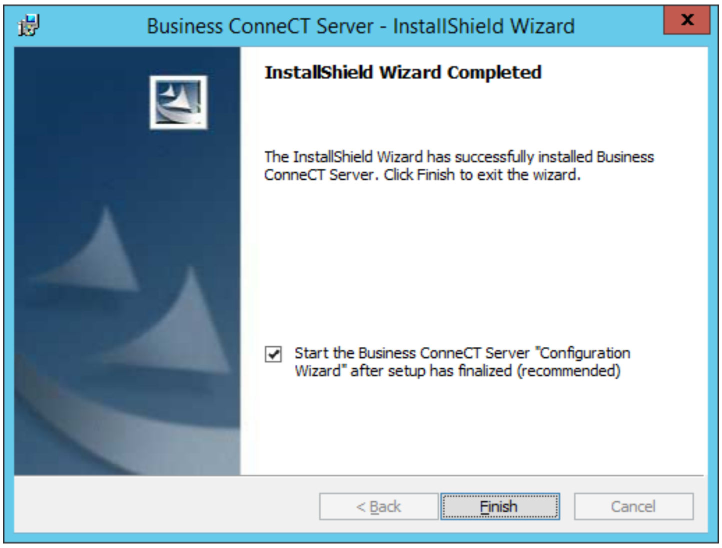
Status:

Copying new files

File: UDP.Communication.dll

Figure 7-10 Installing window

15. When the installation is finished, the “InstallShield Wizard completed”-window appears.


Business ConneCT Server - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Business ConneCT Server. Click Finish to exit the wizard.

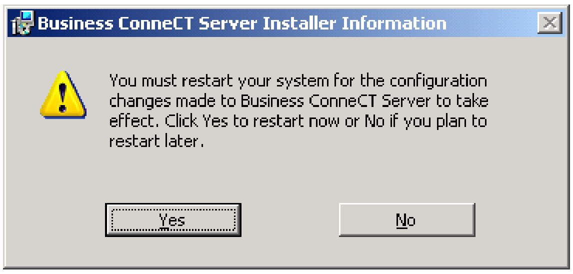
☑ Start the Business ConneCT Server "Configuration Wizard" after setup has finalized (recommended)

Figure 7-11 Installation completed window

Mark the **Start the** “**Configuration Wizard**” **after setup has finalized** check box and click **Finish**. The check box does not appear during upgrading of an existing BCT system.

Note: *Finalizing the installation may take a while, be patient with the system.*

16. When asked to restart,



Business ConneCT Server Installer Information

You must restart your system for the configuration changes made to Business ConneCT Server to take effect. Click Yes to restart now or No if you plan to restart later.

click **Yes**. When the PC is restarted the Configuration Wizard will start.

Note: *During an installation, services related to BCT are stopped. When other applications are still running on the server, they might have dependencies to the BCT services. The BCT install is not able to stop a service that has a dependency to other/unknown services. When the installation remains a long time at '**stopping services**', you should look at the list of services and see which service is in 'stopping' mode. Stop (or Kill) the service in stopping mode or the dependent service(s). If the service is stopped the installation should continue.*

Note: *If you enable the **Windows Firewall** after installing BCT, make sure you run the Security Configurator to set the specific firewall port exceptions, and then reboot the server. See 8.1.2 Security settings.*

Note: *When switching domains (also e.g. from workgroup to domain), then the firewall settings may need to be set again. You can use the Security Configurator (in the Tools menu of the BCT start menu entry). See 8.1.2 Security settings.*

Note: *When you experience problems during installation and support is required please include the setup log file named 'BusinessConneCT-Server_yyyymmddhhmmss' located in folder C:\Program Files (x86)\Common Files\NEC\Setup Log Files'*

7.1. Uninstalling BCT

The application and all the supporting modules can be uninstalled via **Start > Control Panel> Add or Remove Programs.**

7.2. Upgrading BCT

For information on how to upgrade, please refer to the related Release Notes which can be found on the DVD under D:\Business ConneCT Resources\Documentation.

8. SERVER CONFIGURATION

8.1. Generic configuration

8.1.1. Using the Configuration Wizard

Use the Configuration Wizard to configure BCT for a *stand-alone PBX*, an operator and/or Contact Center configuration. For more complex configurations use the BCT System Settings and the BCT Supervisor Dashboard.

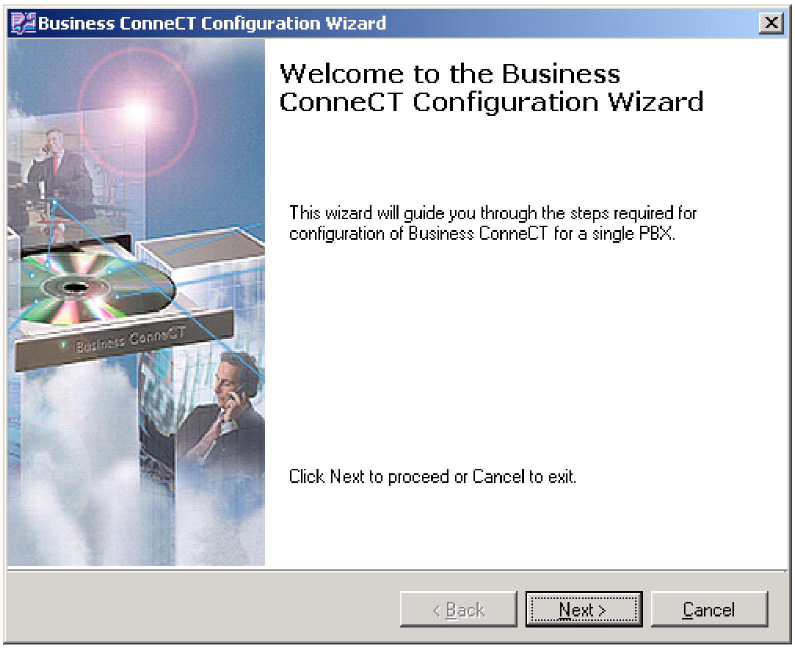
If you need to modify the configuration, you can use the Configuration Wizard again to modify the desired items. However, when the configuration is too complex or too many changes have been made, the Configuration Wizard will not start. You will get the warning message “Incompatible Configuration Detected”. In that case, use the BCT System Settings or the BCT Supervisor Dashboard to make changes.

Note: for UNIVERGE 3C server systems having Open Numbering Plan enabled, the Configuration Wizard cannot be used to initially create the PBX, use BCT System Settings instead. However when the PBX is synchronized for the first time, the Configuration Wizard can be used afterwards to configure VMP lines, Routing Points, operator and agent routers etc.

Note: *All possible steps of the Configuration Wizard are described here. In your case, the Configuration Wizard will skip some steps, depending on the type of PBX that you have.*

1. Start the Configuration Wizard. Either select the option at the end of the install program, or go to Start/Program Files (x86)/Business ConneCT/Tools and select Configuration Wizard.

2. After a prepare dialog the welcome screen of the Configuration Wizard appears.



Business ConneCT Configuration Wizard

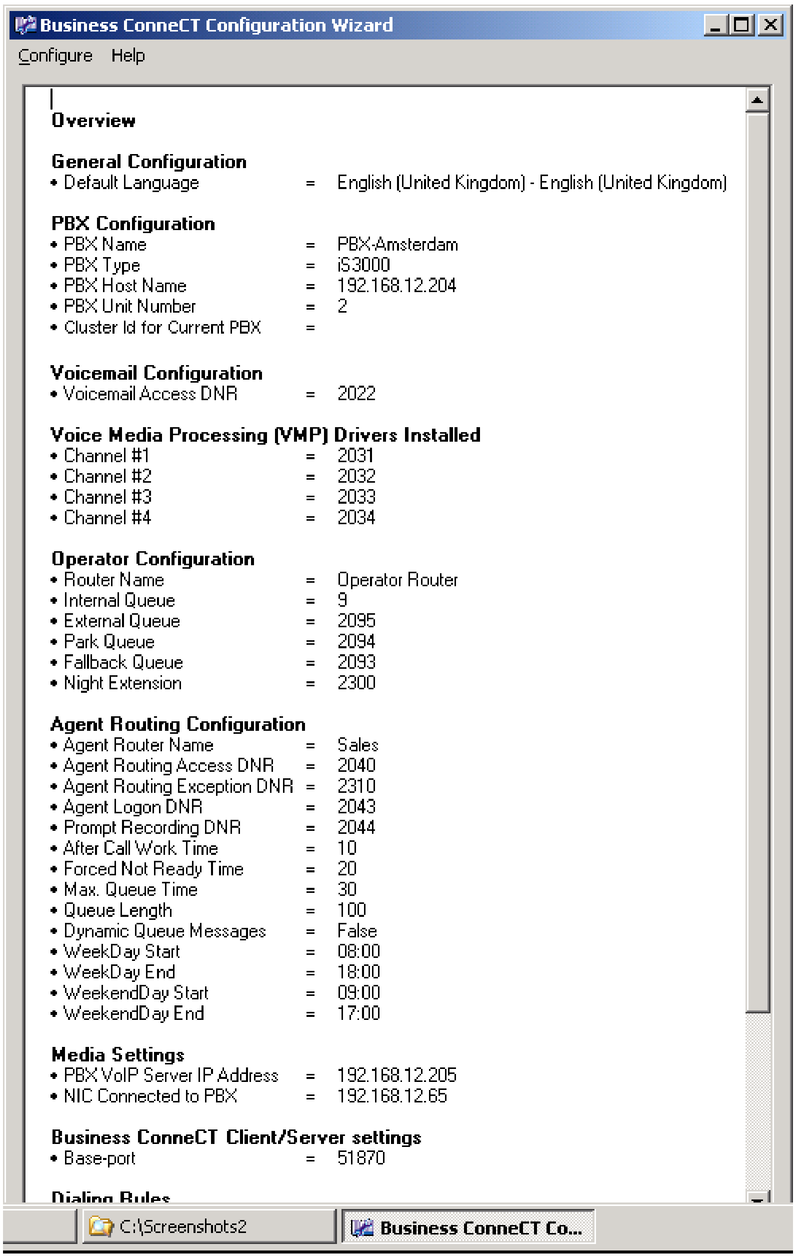
Welcome to the Business ConneCT Configuration Wizard

This wizard will guide you through the steps required for configuration of Business ConneCT for a single PBX.

Click Next to proceed or Cancel to exit.

Figure 8-1 Configuration Wizard welcome screen

If you already used the Configuration Wizard, you will get the following screen:



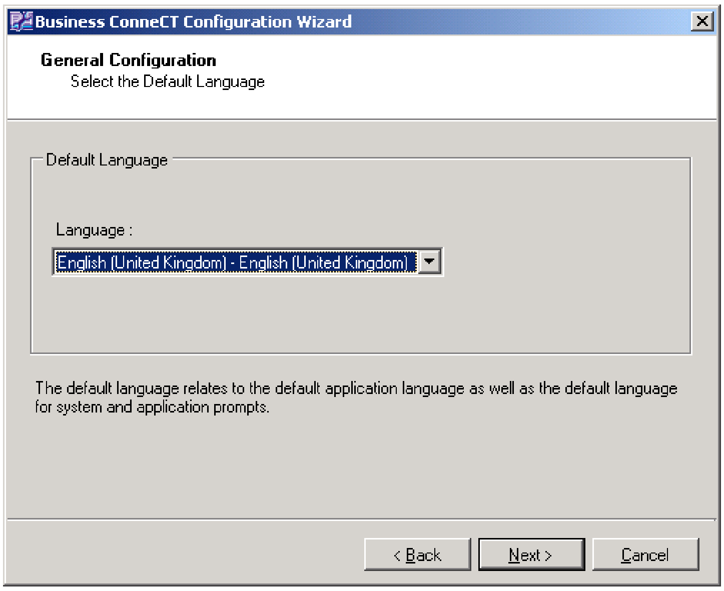
```
Overview

General Configuration
• Default Language               =   English (United Kingdom) - English (United Kingdom)

PBX Configuration
• PBX Name                       =   PBX-Amsterdam
• PBX Type                       =   iS3000
• PBX Host Name                  =   192.168.12.204
• PBX Unit Number                =   2
• Cluster Id for Current PBX     =

Voicemail Configuration
• Voicemail Access DNR           =   2022

Voice Media Processing (VMP) Drivers Installed
• Channel #1                     =   2031
• Channel #2                     =   2032
• Channel #3                     =   2033
• Channel #4                     =   2034

Operator Configuration
• Router Name                    =   Operator Router
• Internal Queue                 =   9
• External Queue                 =   2095
• Park Queue                     =   2094
• Fallback Queue                 =   2093
• Night Extension                =   2300

Agent Routing Configuration
• Agent Router Name              =   Sales
• Agent Routing Access DNR       =   2040
• Agent Routing Exception DNR    =   2310
• Agent Logon DNR                =   2043
• Prompt Recording DNR           =   2044
• After Call Work Time           =   10
• Forced Not Ready Time          =   20
• Max. Queue Time                =   30
• Queue Length                   =   100
• Dynamic Queue Messages         =   False
• WeekDay Start                  =   08:00
• WeekDay End                    =   18:00
• WeekendDay Start               =   09:00
• WeekendDay End                 =   17:00

Media Settings
• PBX VoIP Server IP Address     =   192.168.12.205
• NIC Connected to PBX           =   192.168.12.65

Business ConneCT Client/Server settings
• Base-port                      =   51870

Dialing Rules
```

Figure 8-2 Configuration overview screen

In that case you must select Configuration Wizard from the Configure menu, to get the welcome screen.

Click **Next** in the Welcome screen.

3. The “Default Language”-window appears.



Business ConneCT Configuration Wizard

General Configuration
Select the Default Language

Default Language

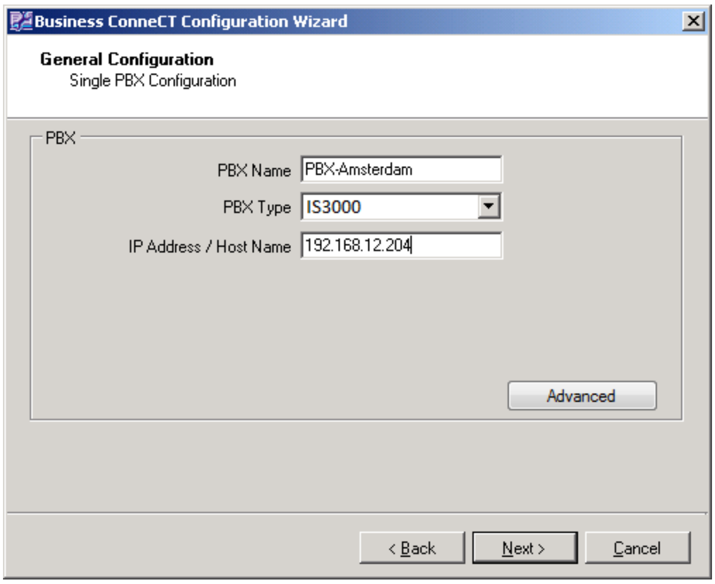
Language : English (United Kingdom) - English (United Kingdom)

The default language relates to the default application language as well as the default language for system and application prompts.

Figure 8-3 Select Default Language screen

Select the required language for the application and prompts and click **Next**.

4. The first “PBX configuration”-window appears.



Business ConneCT Configuration Wizard

General Configuration
Single PBX Configuration

PBX

PBX Name: PBX-Amsterdam

PBX Type: IS3000

IP Address / Host Name: 192.168.12.204

Figure 8-4 PBX Configuration screen

Note that some fields may or may not be shown, or may be presented in a separate window, depending on the PBX type.

Enter the required information:

- Enter the **PBX Name** and **PBX Type**.
- Enter the IP address / Host name

PBX:	**IP address/Host name of the PBX:**
SV8500 /SV9500	LAN2 (ACT) IP address
iS3000	CPU3000, CPU4000 or CIE board
SV8100 /SV9100	VoIP board
SV9100-TAPI	Voip board
SV8300 /SV9300	VoIP board
UNIVERGE 3C	UNIVERGE 3C system

For UNIVERGE 3C some additional fields are required:

- **Port Number**: port that is used for UNIVERGE 3C web service, see 2.4.1 Port usage (UNIVERGE 3C CTI port).
- **Domain Name**: the fully specified domain name is required to connect to Active Directory.
- **Username**: the user should be the CTIuser AD user account, created as described in sections
  4.6.2.1 How to create a CTIuser account and 4.6.4.9 Configure CTIuser.

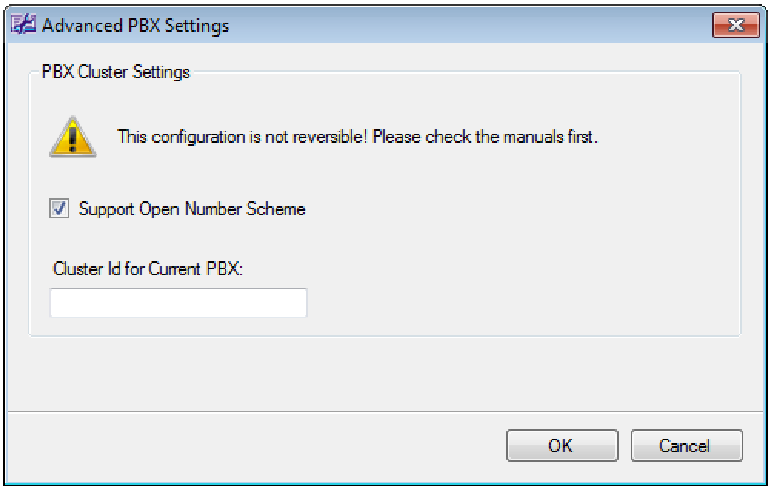
Note: *For the PBX types SV8100/SV9100 and UNIVERGE 3C, the license is based on using the PBX as license server. In that situation the checkmark "Use as license server" in the Single PBX Configuration screen must be set.*

5. Depending on the type of PBX, some of the following fields are disabled:

- **Requires Authentication**: you may need to select this box before you can use the Username and Password fields.

- **Password**: this is the password that is used by the PBX user administrator. The default SV8100/SV9100 is user1 with password 1111. The default for AspireX/AspireUX is USER1 with password 1111. Note that user name is case sensitive.

- **Advanced**: If the PBX has not yet been synchronized successfully, the **Advanced** button is enabled. If you Click on it, the Advanced PBX Settings window is displayed:


Advanced PBX Settings

PBX Cluster Settings

This configuration is not reversible! Please check the manuals first.

☑ Support Open Number Scheme

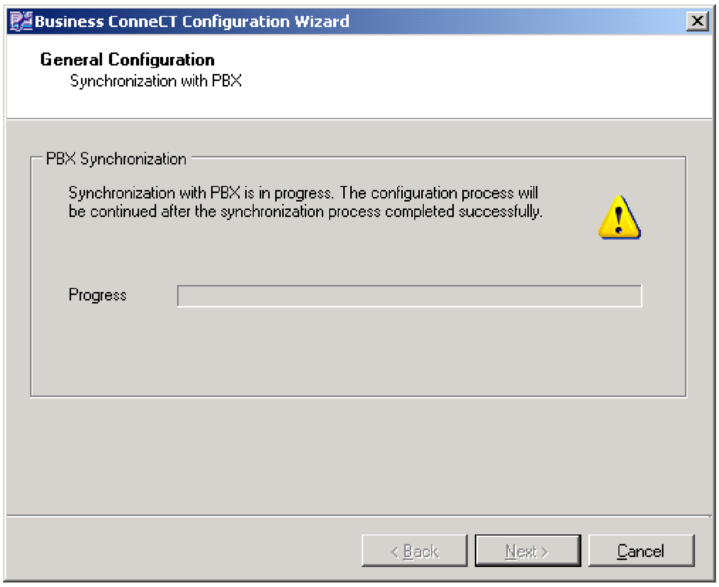
Cluster Id for Current PBX:

Figure 8-5 Advanced PBX Settings

By default Open Number Scheme is not supported. Click on Support Open Number Scheme to change that. You have the possibility to define whether the current (first) PBX should be put in a cluster that supports Open Number Scheme (enter cluster id in Cluster Id for Current PBX) or in a cluster that supports Closed Number Scheme (leave Cluster Id for Current PBX empty).
Click on **OK**.

Click **Next**.

6. The “Synchronization with PBX”-window appears and the Configuration Wizard starts synchronizing.



General Configuration
Synchronization with PBX

PBX Synchronization

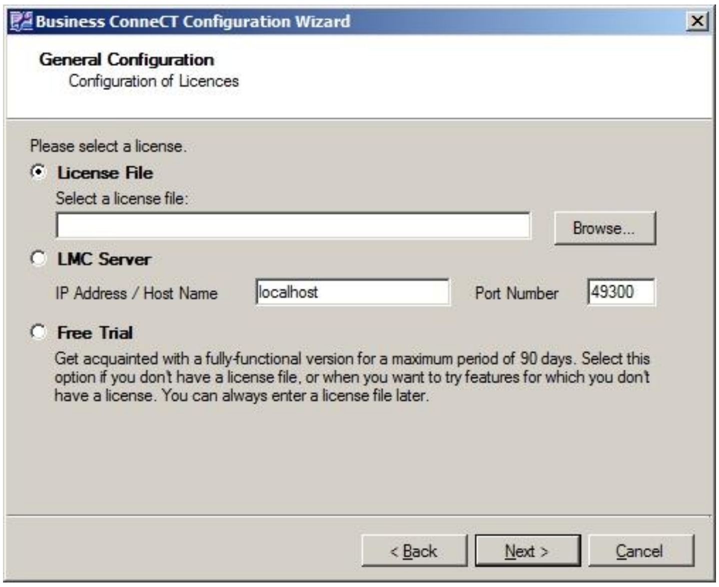
Synchronization with PBX is in progress. The configuration process will be continued after the synchronization process completed successfully.

Progress

Figure 8-6 PBX Synchronization in progress screen

Wait until this is completed. Be patient, Synchronization might take some time. When Synchronization is completed successfully, click **Next**.

7. The license window appears.



General Configuration
Configuration of Licences

Please select a license.

● License File

Select a license file:

○ LMC Server

IP Address / Host Name: localhost   Port Number: 49300

○ Free Trial

Get acquainted with a fully-functional version for a maximum period of 90 days. Select this option if you dont have a license file, or when you want to try features for which you dont have a license. You can always enter a license file later.

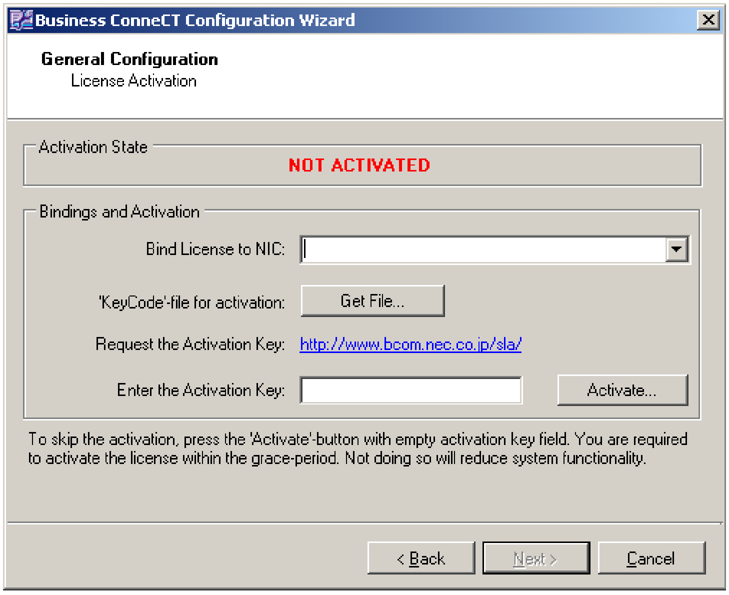
Figure 8-7 Configuration of licenses screen

If you use the LMC to obtain licenses, select **LMC Server**, and fill in the **IP Address / Host Name**. The default port number has been filled in already.

Click **Next**.

Note: *For the PBX types SV8100/SV9100 and UNIVERGE 3C (US), the license is based on using the PBX as license server. In that situation the checkmark "Use as license server" in the PBX Configuration screen must be set.*

8. The license activation window appears (only in case of Japanese Domestic license file):



NOT ACTIVATED

http://www.bcom.nec.co.jp/sla/

To skip the activation, press the 'Activate'-button with empty activation key field. You are required to activate the license within the grace-period. Not doing so will reduce system functionality.

Figure 8-8 License Activation Screen

Note: *It is possible to postpone the activation step. In that case leave the input field '**Enter the Activation Key'** empty and press the '**Activate'**-button. As result the '**Next**'-button will be enabled.*

Please remember that the Business ConneCT license has to be activated within 30 days! BCT license activation can be done via the BCT Configuration Wizard or via the BCT License Manager (**Start > Business ConneCT > Tools**)

Execute next steps:

a) Select the Network Card (NIC) to which the license will be bound to.

Note: *Removing or changing the NIC afterwards will de-activate the license. In that case the license has to be activated again within 30 days.*

b) Get the 'KeyCode'-file (`KEYCODE.act`), which is required to retrieve the **Activation Key** in the next step. The KeyCode-file contains information about your license file and the selected NIC.

c) Visit the **Japanese License Center** internet page by pressing the link (the page will open in default web-browser).
At the License Center internet page: log in into your account, and go to your product page for retrieving the Activation Key. You will be asked for the 'KeyCode'-file.

__Note:__ You can also visit the site using another PC/Laptop; it is not mandatory to do this from the BCT Server PC. However, in that case you will need to transfer the 'KeyCode'-file to this other PC and take over the Activation Key.

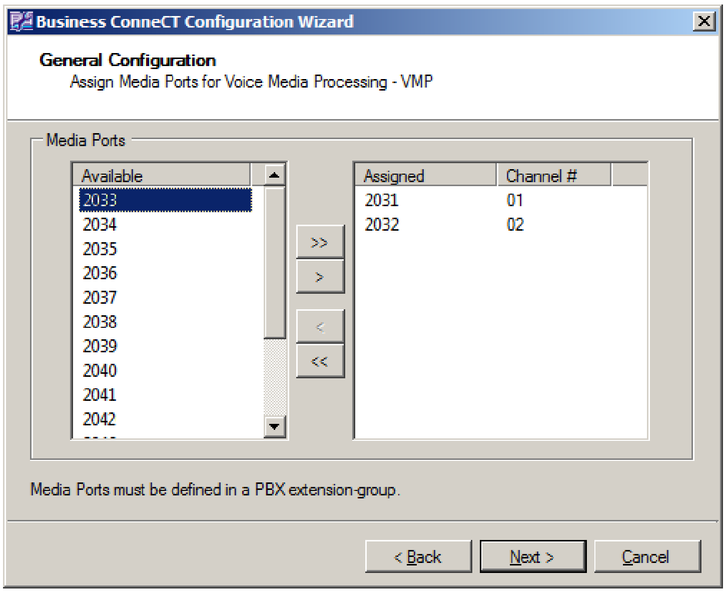
d) Enter the Activation Key, as represented on the internet page, in the input field "**Enter the Activation Key**" and press the "**Activate**"-button. In case of valid activation, the activation state on top of page will change to green "ACTIVATED".

Click **Next.**

9. If required for your PBX type, the "Special Monitored Number"-window appears. Please refer to the relevant PBX chapter for more information.

Select the number and click **Next**.

10. The "Media Ports"-window appears.



Business ConneCT Configuration Wizard

General Configuration

Assign Media Ports for Voice Media Processing - VMP

Media Ports

Available
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042

Assigned	Channel #
2031	01
2032	02

Media Ports must be defined in a PBX extension-group.

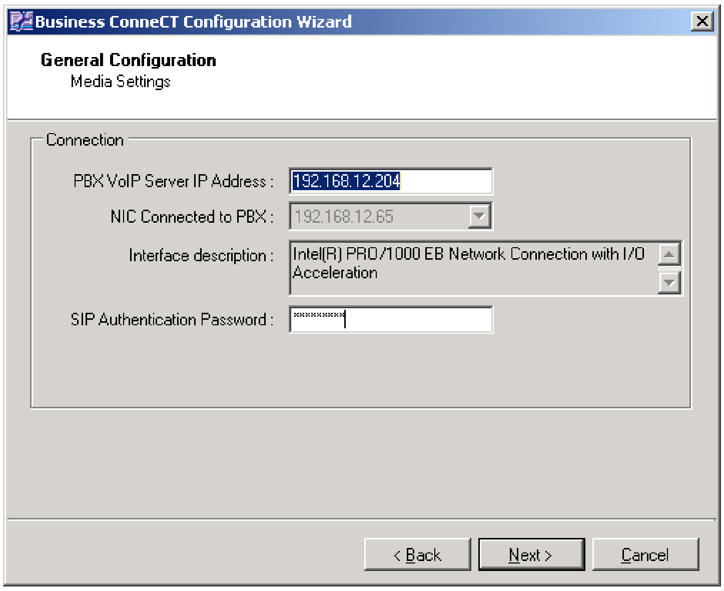
Figure 8-9 Assign Media Ports for VMP screen

If you have defined the Media Ports / VMP lines correctly in the department or UCS group in the PBX (see chapter 4.x – x depends on which PBX type you use), the Configuration Wizard detects automatically which extensions are suitable / available as Media Ports.

Select the available Media Ports and press '>' to assign them as VMP line. The channel number is assigned incrementally by the Configuration Wizard.

Click **Next.**

11. If VMP is selected during installation, the following window appears:



General Configuration

Media Settings

Connection

PBX VoIP Server IP Address : 192.168.12.204

NIC Connected to PBX : 192.168.12.65

Interface description : Intel(R) PRO/1000 EB Network Connection with I/O Acceleration

SIP Authentication Password : **********

Figure 8-10 VMP Media Settings page

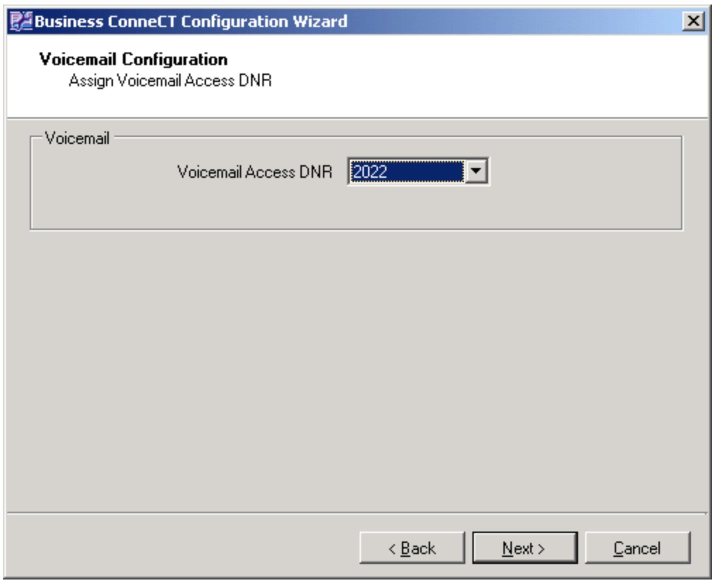
Enter:

- the IP address of the VoIP card (applicable for SV8100/SV9100 / AspireX/AspireUX)
- the IP address of the BCT server (applicable for SV8300/SV9300 / SV8500/SV9500).
  Note that this is the IP address on the BCT server side, which is connected via the network to the PBX VOIP card.
- the SIP-Server IP address (applicable for iS3000)
  For SIP@Net, the Secure Media (TLS+sRTP) option can be selected.
- the UNIVERGE 3C Server address (UNIVERGE 3C).
  For UNIVERGE 3C, the Secure Media (TLS+sRTP) option can be selected.
- You can enter a password for secured SIP authentication on all VMP IVR-lines.

The “Interface”-field is the IP address used to interface to the PDS-Server, to the SIP-Server or to the UNIVERGE 3C System.

When you return to the Configuration Wizard, click **Next**.

12. The “Voicemail Configuration”-window appears.



Voicemail Configuration
Assign Voicemail Access DNR

Voicemail

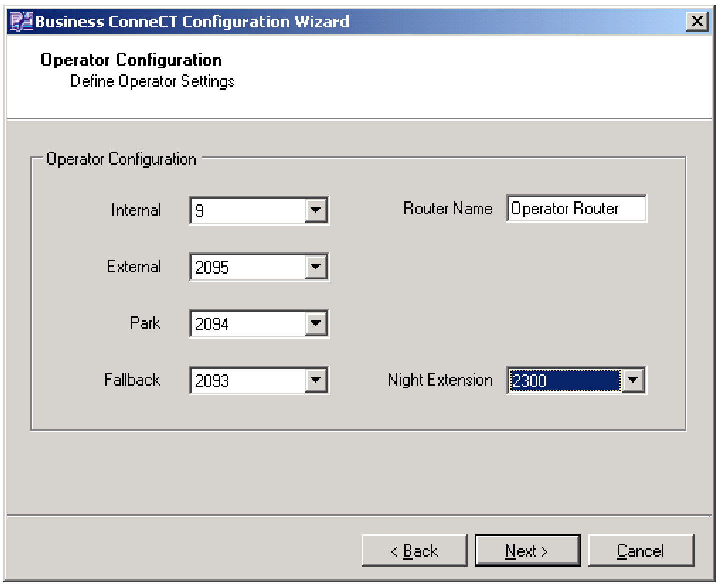
Voicemail Access DNR: 2022

Figure 8-11 Assign Voicemail access DNR screen

The Voicemail Access DNR has been defined in the PBX (see chapter 4.x – x depends on which PBX type you use).

Select the correct voicemail access number from the drop down list and click **Next**.

13. The “Operator Configuration”-window appears.



Operator Configuration
Define Operator Settings

Operator Configuration

Internal: 9

External: 2095

Park: 2094

Fallback: 2093

Router Name: Operator Router

Night Extension: 2300

Figure 8-12 Define Operator Settings screen

If you have defined the DNRs associated to the Operator queues, and Night Extension correctly in the PBX (see chapter 4.x – x depends on which PBX type you use), the Configuration Wizard detects automatically which DNRs are suitable / available.

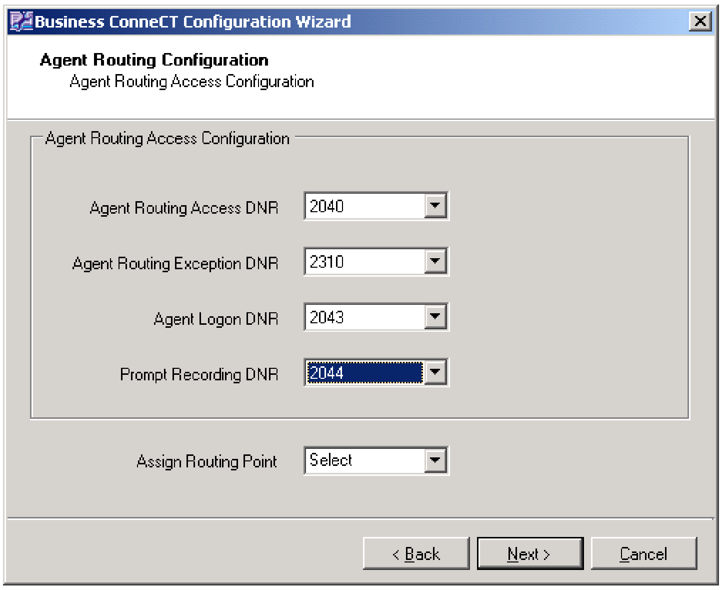
Select the Queue numbers.

Enter the operator **Router Name**.

Select the operator **Night Extension**.

Click **Next**.

14. The “Agent Routing Access Configuration”-window appears.



Business ConneCT Configuration Wizard

Agent Routing Configuration

Agent Routing Access Configuration

Agent Routing Access Configuration

Agent Routing Access DNR: 2040

Agent Routing Exception DNR: 2310

Agent Logon DNR: 2043

Prompt Recording DNR: 2044

Assign Routing Point: Select

Figure 8-13 Agent Routing Access Configuration screen

The DNRs have been defined in the PBX (see chapter 4.x – x depends on which PBX type you use).

Select the Agent Routing Access DNR.

Select the Agent Routing Exception DNR.

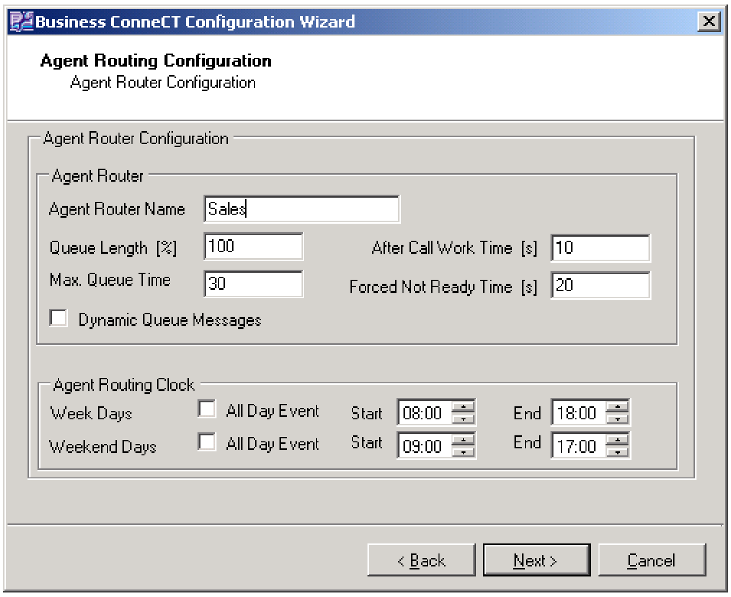
Select the Agent Logon DNR.

Select the Prompt Recording DNR.

Assign Routing Point: Assigning at least one routing point is for most PBX types required, because the system has to be able to put a call on hold via a routing point.

Click **Next**.

15. If the BCT Contact Center part is used, the “Agent Router Configuration”-window appears.



Agent Routing Configuration
Agent Router Configuration

Agent Router Configuration

Agent Router

Agent Router Name: Sales

Queue Length [%]: 100

After Call Work Time [s]: 10

Max. Queue Time: 30

Forced Not Ready Time [s]: 20

□ Dynamic Queue Messages

Agent Routing Clock

Week Days □ All Day Event Start 08:00 End 18:00

Weekend Days □ All Day Event Start 09:00 End 17:00

Figure 8-14 Agent Router Configuration screen

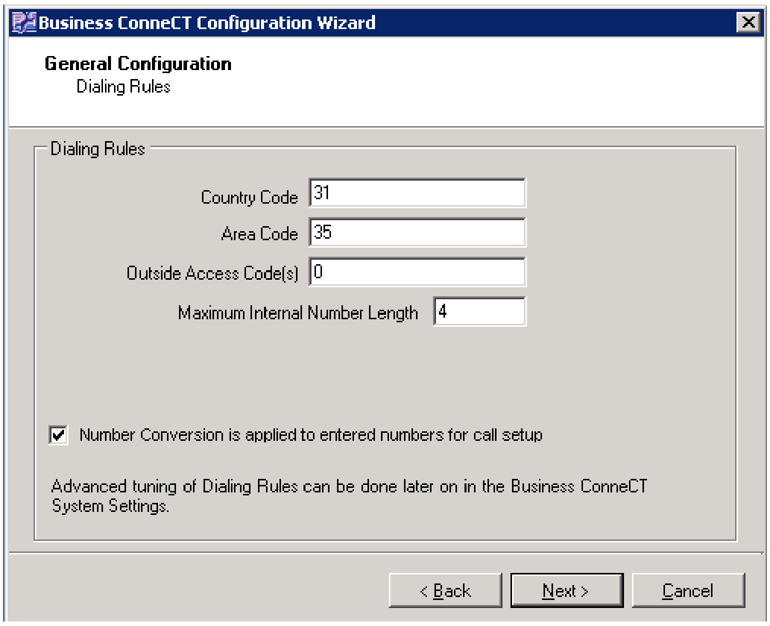
Select the following:

- Agent Router Name (plus QueueTime, QueueLength, ForcedNotReadyTime, ACWTime);
- Agent Routing Clock Times (week days + weekend days);
- Agent Routing Exception Destination.

Click **Next**.

Note: *The Base port number is by default 51870 and doesn't need to be changed unless another application is using the same portnumber (see 8.1.6.8 Media Ports Configuration)*

16. The “Dialing Rules”-window appears.



General Configuration
Dialing Rules

Dialing Rules

Country Code: 31

Area Code: 35

Outside Access Code(s): 0

Maximum Internal Number Length: 4

☑ Number Conversion is applied to entered numbers for call setup

Advanced tuning of Dialing Rules can be done later on in the Business ConneCT System Settings.

Figure 8-15 Dialing Rules window

For more information see 18 Appendix H – DIALING RULES AND NUMBER CONVERSION.

The dialing rules define in which area (and country) your PBX is located, and some of the internal parameters used in handling telephone numbers. Usually you need only one set of dialing rules, which defines the "Default Area". You can specify additional areas, see 8.1.11 Dialing Rules, if needed.

Here you define the Default Area.

- Country Code – see note below

- Area Code
  Note: Fill in the Area Code as presented in the international number format, usually without the National Access Code. For countries where local numbers include the Area Code, this field must be left empty.

- Outside access code(s). The first code is used by BCT used for outside access.
  Note: You can specify a (comma separated list). Any other codes can be used by the PBX.

- Maximum internal number length

- Option "Number conversion is applied to entered numbers for call setup"
  This applies only to telephone numbers entered manually by a user to make a call (default = activated).

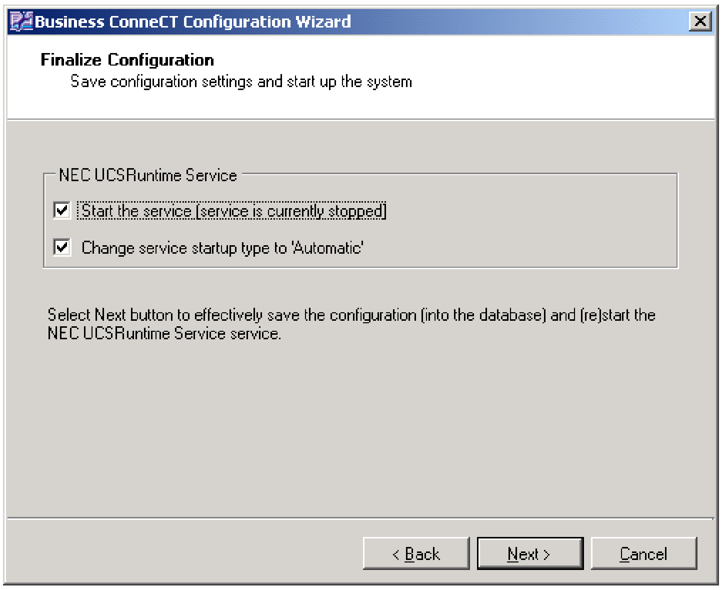
  Note: *If this option is deactivated, then the user must enter dialable numbers, so include outside access code and area code, if required. Deactivating this option may be required if there is (substantial) overlap between internal numbers and local numbers.*

Click **Next**.

Note: *Trunk access codes: For a number of PBX types, numbers over the trunk lines must be prefixed with an access code to get correct phone number information. See 18.3.2 Trunk Line access codes whether this is the case for your PBX.*

Note: *When you have entered the **Country Code**, the national number plan of that country is available in BCT, provided that the country is supported in the Dialing Rules. A list of supported countries can be found in the BCT Boundary Specification.*
When your country is not in this list, only basic conversions are done, like removing non-dialable digits and adding national and international prefixes. To ensure correct number conversion, please contact the support desk.

17. The Finalize Configuration window appears.



Business ConneCT Configuration Wizard

Finalize Configuration

Save configuration settings and start up the system

NEC UCSRuntime Service

☑ Start the service (service is currently stopped)

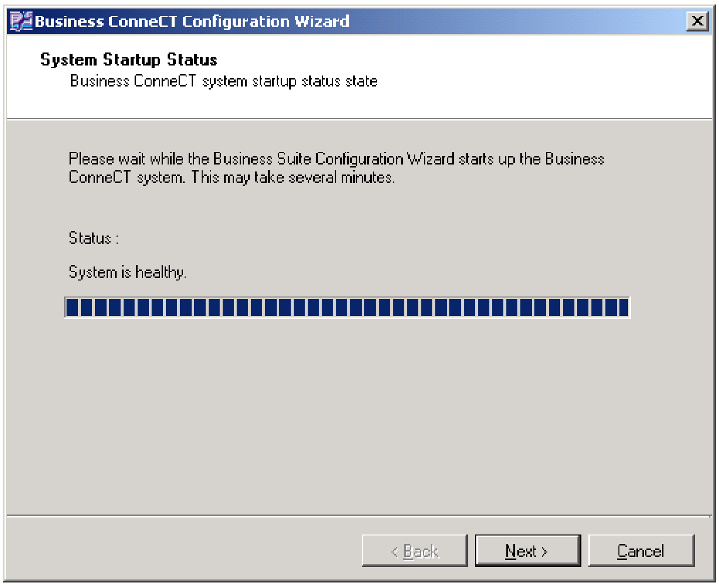
☑ Change service startup type to 'Automatic'

Select Next button to effectively save the configuration (into the database) and (re)start the NEC UCSRuntime Service service.

Figure 8-16 Finalize Configuration window

Mark the check boxes and click **Next**.

18. The “System Startup Status”-window appears. When this is ready, click **Next**.



Business ConneCT Configuration Wizard

System Startup Status

Business ConneCT system startup status state

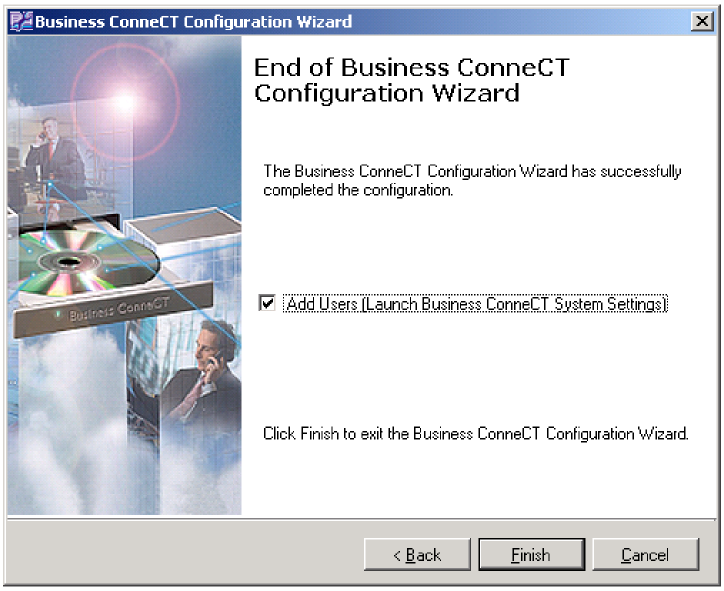
Please wait while the Business Suite Configuration Wizard starts up the Business ConneCT system. This may take several minutes.

Status :

System is healthy.

Figure 8-17 System Startup status screen

19. The “End of Configuration Wizard”-window appears.



End of Business ConneCT Configuration Wizard

The Business ConneCT Configuration Wizard has successfully completed the configuration.

☑ Add Users (Launch Business ConneCT System Settings)

Click Finish to exit the Business ConneCT Configuration Wizard.

Figure 8-18 Successfully completed screen

Mark the "Add/Modify Users (Launch Directory Browser)"-check box if you want to start importing users.

Click **Finish**.

The data you entered is imported into the BCT database, and then the configuration overview is presented. See Figure 8-2 Configuration overview screen.

8.1.2. Security settings

Network security

After installing BCT, you must set the server security policies to match the network's security policy. BCT includes the Operating System Security Configurator tool. If required, use this tool to enable BCT related programs and services in combination with the Windows Firewall.

See sections about Windows Firewall Configuration below.

In case a 3rd party security kit is used, combining virusscanner and firewall, then the Windows Firewall will be disabled. In that case you need to add the BCT processes in the exclusion list (or trusted applications) of the 3rd party firewall. See 8.1.2.4 3rd Party Firewall configuration.

Note: *Programs like Backup tools or Virusscanners (scanning process, but also virusscan updates) can be so intensive, that the real-time handling of BCT cannot be guaranteed. So it is advised to perform these actions in low traffic hours.*

Public access to BCT web pages

When a customer wants some BCT functionality to be available from outside the company network, the BCT Server is placed in the DMZ. By default all BCT web pages and folders are then publicly accessible from the internet. To protect against unauthorized access see chapter 22 Appendix L – HOW TO LIMIT PUBLIC ACCESS TO BCT WEB PAGES AND WEB APPLICATIONS.

Other generic security related topics

For generic security related topics see white paper [Securing BCT Web Application] in 1.1 References

8.1.2.1. Windows Firewall configuration - Remote SQL Server access

When the SQL Server is running on a server where the Windows Firewall is turned on, you need to enable (allow) remote access in case:

- SQL Server is installed on a dedicated remote server PC or when
- SQL Server is installed and running on BCT server and access is required by BCT Contact Center Client.

When the SQL Server default instance is used by default it will listen on the fixed TCP port 1433.

This port should be opened in the firewall. However, when using a SQL Server named instance, you should first configure the Database Engine to listen on a specific port known as fixed port or static port. By default a named instance will listen on dynamically defined ports. After configuration this fixed TCP port should be opened in the firewall.

To configure the SQL Server to listen on a specific port, use procedure below:

Preconditions:

1. Make sure that the computers are registered in the same domain.

Actions:

1. In SQL Server Configuration Manager, expand **SQL Server Network Configuration**, and then click on the server instance you want to configure.
2. In the right pane, double-click **TCP/IP**.
3. In the **TCP/IP Properties** dialog box, click the **IP Addresses** tab.
4. In the **TCP Port** box of the **IPAll** section, type an available port number. For example 49172 (should be in range from 49152 through 65535, see http://www.iana.org).
5. Click **OK** to close the dialog box, and click **OK** to the warning that the service must be restarted.
6. In the left pane, click **SQL Server Services**.
7. In the right pane, right-click the instance of SQL Server, and then click **Restart**. When the Database Engine restarts, it will listen on the defined fixed TCP port.

Notes:

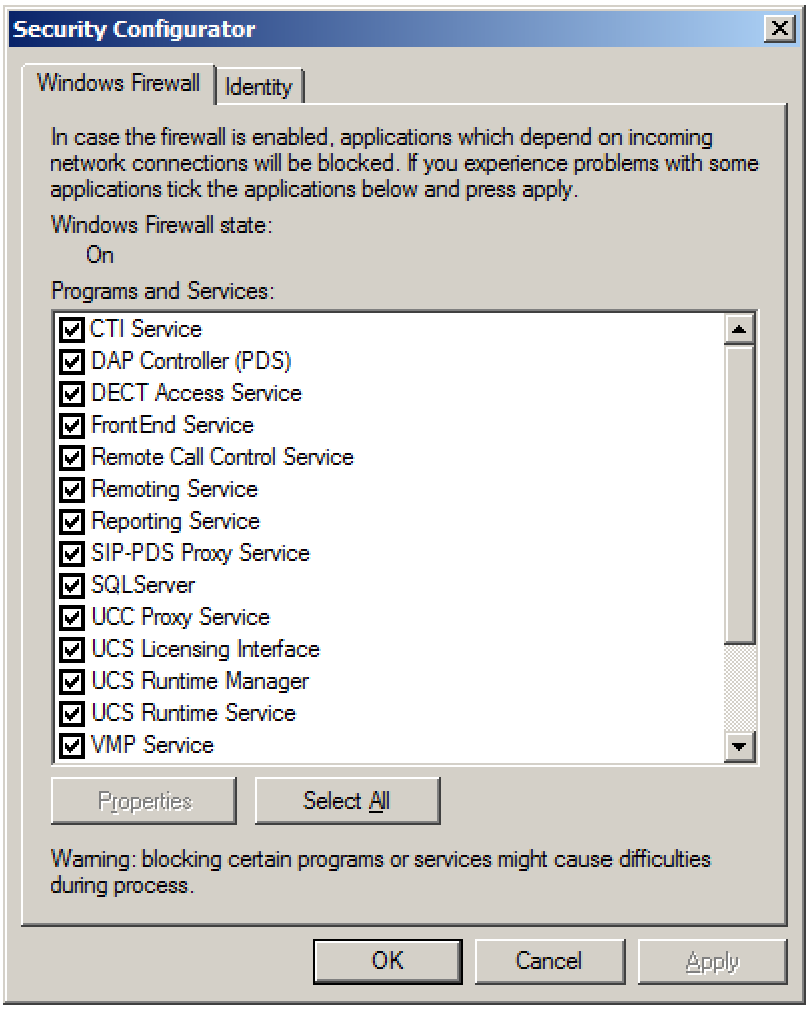
- *For detailed information about SQL Server aspects when running on another server see Microsoft documentation (e.g. http://msdn.microsoft.com/en-us/library/ms345343(v=sql.105).aspx).*
- *You should enable the protocols ‘TCP/IP’ and ‘Named Pipes’ on the remote SQL Server database engine.*
- *To connect to SQL Server named instance using computer name and instance name the SQL Server Browser service should be running and the UDP port 1434 should be opened in the firewall.*

8.1.2.2. Windows Firewall configuration - Server

Actions:

1. Open the Security Configurator via: Start\Programs\Business ConneCT\Tools\Security Configurator

2. After starting the Security Configurator, the Windows Firewall tab shows:



In case the firewall is enabled, applications which depend on incoming network connections will be blocked. If you experience problems with some applications tick the applications below and press apply.

Windows Firewall state:
On

Programs and Services:

- ☑ CTI Service
- ☑ DAP Controller (PDS)
- ☑ DECT Access Service
- ☑ FrontEnd Service
- ☑ Remote Call Control Service
- ☑ Remoting Service
- ☑ Reporting Service
- ☑ SIP-PDS Proxy Service
- ☑ SQLServer
- ☑ UCC Proxy Service
- ☑ UCS Licensing Interface
- ☑ UCS Runtime Manager
- ☑ UCS Runtime Service
- ☑ VMP Service

Warning: blocking certain programs or services might cause difficulties during process.

Figure 8-19 BCT related programs and services that are affected by Windows Firewall

3. Set all check boxes for the BCT related programs and services to enable them. If no Windows Firewall is present it will show on the top of the screen, the list will be grayed out, no action is necessary.

***Note**: The "Identity" tab is not used for BCT.*

8.1.2.3. Windows Firewall configuration - Client

The following ports should be open in the firewall (added to exception list) for proper client behavior. Please configure this prior to install of client (to prevent Windows Firewall security alerts).

- UDP – Ports 51871..51873 (or higher)

Refer to 2.4.1 Port usage for more details on port numbers.

8.1.2.4. 3rd Party Firewall configuration

In a third party firewall you need to configure which executables and / or ports you need to include in the Firewall exclusion list. In the following list "EXE" indicates an executable and "TCP" indicates a port. (The paths relate to a 64-bit operating system)

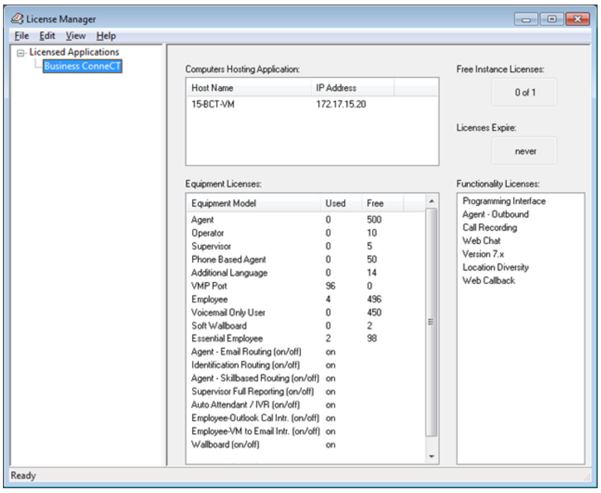
1. CTI Service
   EXE = C:\Program Files (x86)\Common Files\NEC\TSAPI Service\sophocti.exe
2. DAP Controller (PDS)
   EXE = C:\Program Files (x86)\Common Files\NEC\VMP\pds.exe
3. DECT Access Service
   EXE = C:\Program Files (x86)\Common Files\NEC\Services\AccessService.WinService.exe
4. FrontEnd Service
   EXE = C:\Program Files (x86)\Common Files\NEC\Services\FrontEnd.WinService.exe
5. Remoting Service
   EXE = C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe
6. SIP-PDS Proxy Service
   EXE = C:\Program Files (x86)\Common Files\NEC\VMP\SipPdsProxy.exe
7. SQL Server
   TCP= 1433 (note 1)
8. Remote Call Control Service
   EXE = C:\Program Files (x86)\NEC\Remote Call Control\RCC.exe
9. Reporting Service
   EXE = C:\Program Files (x86)\Common Files\NEC\Services\Reporting.Service.WinService.exe
10. Supervisor Dashboard
    EXE = C:\Program Files (x86)\NEC\UCS-Module\Supervisor\Supervisor.exe
11. UCS Licensing Interface
    EXE = C:\Program Files (x86)\NEC\UCS-Module\LM2UCS\LM2UCS.exe
12. UCS Runtime Manager
    EXE = C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRTM.exe
13. UCS Runtime Service
    EXE = C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRuntime.WinService.exe
14. VMP Service
    EXE = C:\Program Files (x86)\Common Files\NEC\VMP\VmpService.WinService.exe
15. Wallboard API
    EXE = C:\Program Files (x86)\NEC\UCS-Module\WallboardService\PhilipsWB_API.exe
16. Wallboard Manager
    EXE = C:\Program Files (x86)\NEC\UCS-Module\WallboardService\PhilipsWBManager.exe
17. Wallboard Service
    EXE = C:\Program Files (x86)\NEC\UCS-Module\WallboardService\PhilipsWBService.exe
18. World Wide Web HTTP
    TCP= 80 (note 1)

Note: *Refer to 2.4.1 Port usage for more details on port numbers.*

8.1.3. Activate BCT licenses

The actions to take to activate BCT licenses depend on the type of License mechanism you use. Each type is described in a separate subchapter. For BCT dongle based licensing please refer to *Appendix R – Dongle Usage (Asian Market Only)*.

When configured correctly it should display as shown in next two example screenshots below. The figure on the right-side is when the License Manager is configured for using LMC.



Computers Hosting Application:

Host Name	IP Address
15-BCT-VM	172.17.15.20

Free Instance Licenses: 0 of 1

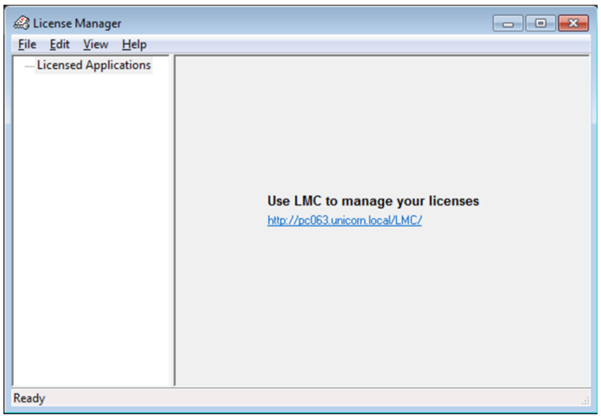
Licenses Expire: never

Equipment Licenses:

Equipment Model	Used	Free
Agent	0	500
Operator	0	10
Supervisor	0	5
Phone Based Agent	0	50
Additional Language	0	14
VMP Port	96	0
Employee	4	496
Voicemail Only User	0	450
Soft Wallboard	0	2
Essential Employee	2	98
Agent - Email Routing (on/off)	on	
Identification Routing (on/off)	on	
Agent - Skillbased Routing (on/off)	on	
Supervisor Full Reporting (on/off)	on	
Auto Attendant / IVR (on/off)	on	
Employee-Outlook Cal Intr. (on/off)	on	
Employee-VM to Email Intr. (on/off)	on	
Wallboard (on/off)	on	

Functionality Licenses:

Programming Interface
Agent - Outbound
Call Recording
Web Chat
Version 7.x
Location Diversity
Web Callback



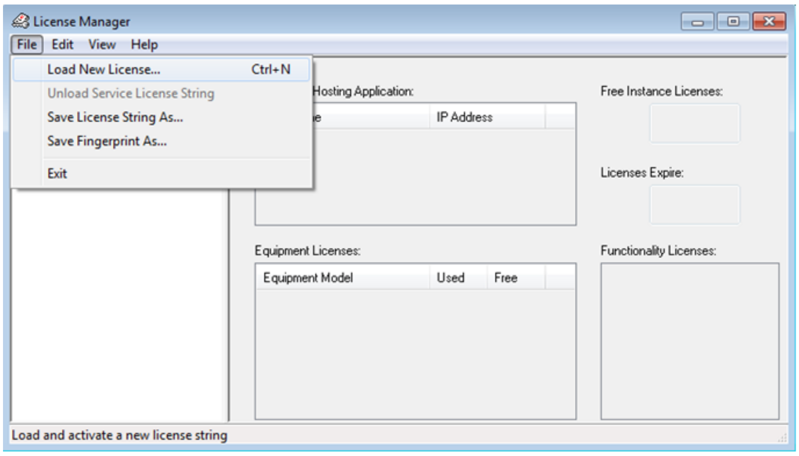
Use LMC to manage your licenses
http://pc063.unicorn.local/LMC/

8.1.3.1. Japanese Domestic License (License File + Activation)

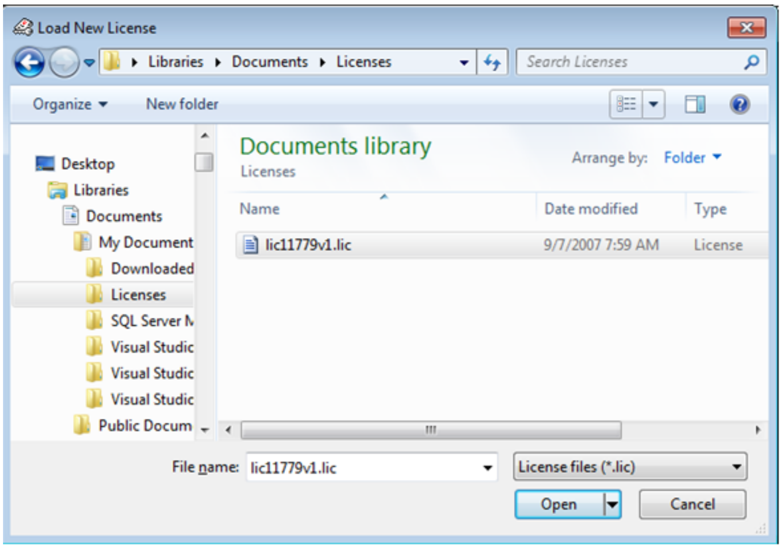
Preconditions:

1. Make sure the License file is available on BCT Server when start loading and activating the license via the License Manager:

   Start via **Start-menu > Programs > Business ConneCT > License Manager**.



Load the License string (File > Load New License). The **Load New License** window will appear:



Name	Date modified	Type
lic11779v1.lic	9/7/2007 7:59 AM	License

File name: lic11779v1.lic

Select the license file and click **Open**

Instead of the License Manager, you can use the Configuration Wizard on first installation (See 8.1.1. Using the Configuration Wizard).

To retrieve the license file (and the Activation Key), please visit your product page at the Japanese License Center website at: http://www.bcom.nec.co.jp/sla (requires log-in).

2. An internet connection is available (either via the BCT Server or another PC/laptop) to visit the Japanese License Center website (http://www.bcom.nec.co.jp/sla) during the Activation phase.
   It is not required that BCT Server should have website access.

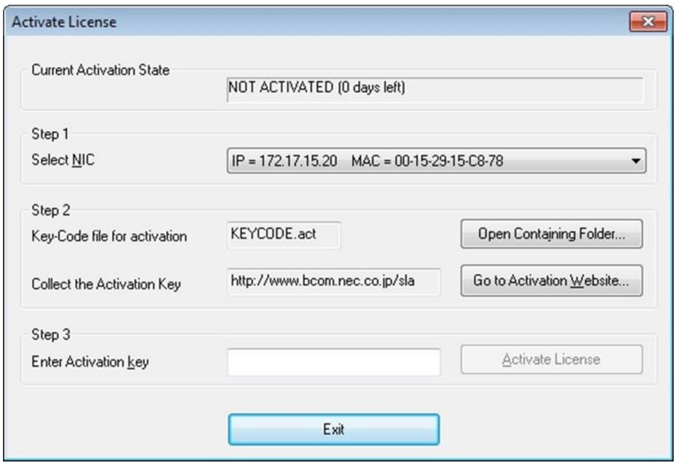
3. The user account information for above website is available

Steps:

1. Start the License Manager via **Start-Menu > Programs > Business ConneCT > Tools > License Manager**.

2. Load the license file via the File-menu.

3. Go to the activation page (menu: Edit > **Activate License**…)



Activate License

Current Activation State: NOT ACTIVATED (0 days left)

Step 1
Select NIC: IP = 172.17.15.20 MAC = 00-15-29-15-C8-78

Step 2
Key-Code file for activation: KEYCODE.act
Collect the Activation Key: http://www.bcom.nec.co.jp/sla

Step 3
Enter Activation key:

4. Select the Network Adapter (NIC) to which the license will be bound to.
   This is required to generate the KeyCode-file, which is used to retrieve the Activation Key.

5. Visit the activation page at the Japanese License Center and provide the KeyCode file (**KEYCODE.act**) in order to retrieve the Activation Key.
   To get the “KEYCODE.act”-file, always use “Open Containing Folder”-button, since this triggers the creation of the file.

6. Back in License Manager, enter this Activation Key and activate it.
   When successful, the current activation state changes to ACTIVATED.

7. Close the License Manager

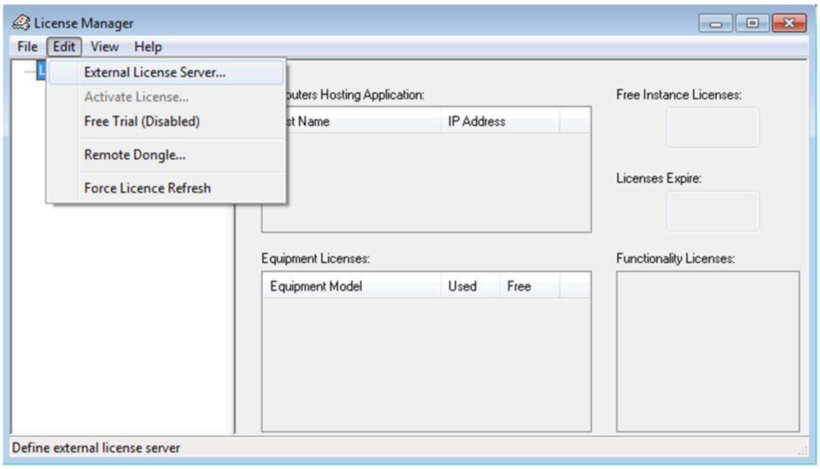
8.1.3.2. External License Server

An external license server may be used, which resides in the PBX, or you may use LMC to manage your license.

Steps:

1. Start the License Manager via **Start-Menu > Programs > Business ConneCT > Tools > License Manager**. The License Manager main window will appear.

2. Open the External License Server Configuration (**Edit** -> **External License Server**):



If you select LMC, see 8.1.3.2.2 Manually refresh / update PBX-based License for further details, otherwise follow the steps in 8.1.3.2.1 PBX-based License.

WARNING: When switching from "Free trial license" to a license mechanism based on PBX licenses or LMC licenses, or visa versa, please always reboot BCT after the change!
Make sure before starting BCT services that not any BCT license is in LMC's "Licenses currently used list"

8.1.3.2.1. PBX-based License

Applies to (SV8100/SV9100 / UNIVERGE 3C)

Preconditions:

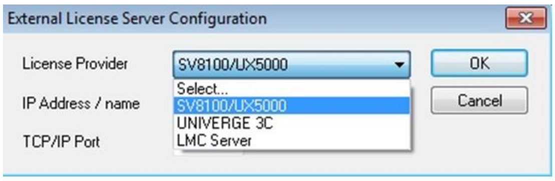
1. PBX-based license for UNIVERGE 3C is only valid for a single BCT server.
   If sharing the licenses for multiple BCT servers, use LMC.

2. In case the license resides in the PBX, the BCT server must already have a connection with the PBX, for instance synchronized with the PBX. The BCT license for the SV8100/SV9100 can be loaded with the feature activation of PCPro.

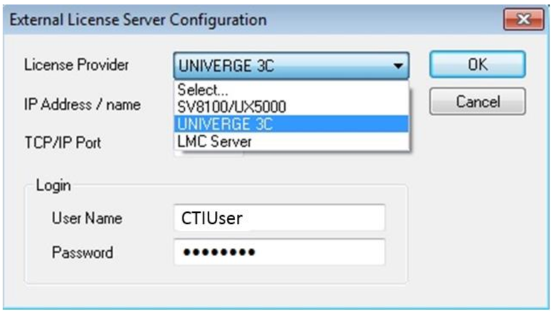
Steps:

1. Open the External License Server Configuration (**Edit** -> **External License Server**).

2. Select the correct PBX-type from the drop down box, and enter the IP address and the Port (the default port is already filled in). In case of 3C, also provide the login credentials


External License Server Configuration

License Provider: SV8100/UX5000


External License Server Configuration

License Provider: UNIVERGE 3C

Login

User Name: CTIUser

Password: ••••••••

3. Close the License Manager.

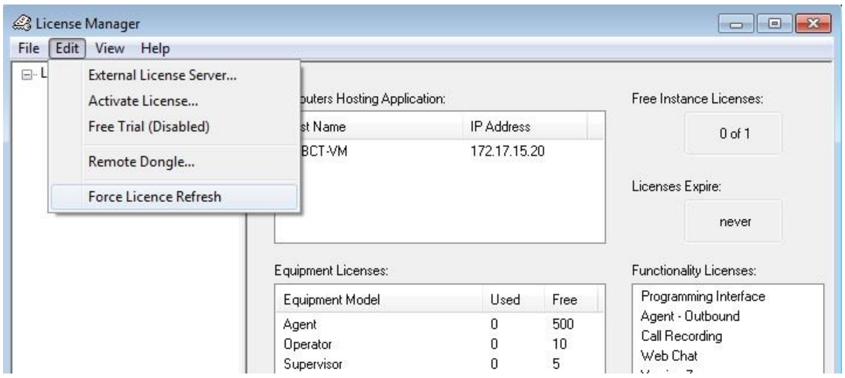
8.1.3.2.2. Manually refresh / update PBX-based License

In the case that the licenses in the PBX have been updated, a manually refresh can be triggered. This forces the License Manager to retrieve the updated licenses immediately instead waiting on its periodical (hourly) checks.

Steps:

1. Start the License Manager via **Start-Menu > Programs > Business ConneCT > Tools > License Manager**. The License Manager main window will appear.

2. Now click on **Edit -> Force License Refresh**



puters Hosting Application:

st Name	IP Address
BCT-VM	172.17.15.20

Free Instance Licenses: 0 of 1

Licenses Expire: never

Equipment Licenses:

Equipment Model	Used	Free
Agent	0	500
Operator	0	10
Supervisor	0	5

Functionality Licenses:

Programming Interface
Agent - Outbound
Call Recording
Web Chat

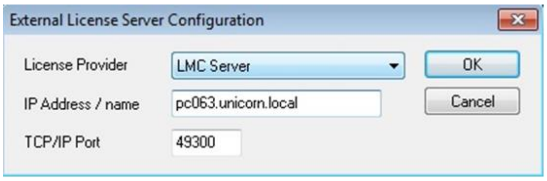
8.1.3.2.3. Use LMC to manage licenses

Preconditions:

1. The LMC has been installed.
Documentation on LMC can be found on the DVD in
D:\Business ConneCT Resources\Optional Packages\License Manager Client\Docs.

Steps:

1. Select the LMC Server, and fill in the IP address. The default port is already filled in.



License Provider: LMC Server

IP Address / name: pc063.unicorn.local

TCP/IP Port: 49300

2. Close the License Manager.

WARNING: When LMC is used, never "ASSIGN' licenses to a BCT Hostname or IP address. BCT will not be able to use such a license and might even refuse to start up!
Make sure before starting BCT services that not any BCT license is in LMC's "Licenses currently used list"

8.1.4. SQL Server memory settings

The memory used by the SQL server that is used by BCT must be limited. This to avoid problems when a lot of users login at the same time. In default installations of SQL server the maximum available memory for SQL = the available RAM memory of the server. To avoid problems the amount of available memory of the SQL server is limited **automatically** during installation.

WARNING: *The Automatic change of the memory properties of an SQL server applies to all users/applications connected to that sql server. The customer MUST BE NOTIFIED if the server is not dedicated for BCT only.*

How to check the memory used by SQL server

Actions:

1. Use SQL Server Management Studio, and search for the SQL server used by BCT in the explorer window on the right. Connect to this SQL server.

2. **Right click** and select **Properties** of the SQL server.

3. Select the **Memory** tab, the correct settings for BCT are: **Dynamically Maximum Server Memory (in MB)**, with a value of at least 512 MB but significantly less than the available RAM memory.

4. Press **OK**

8.1.5. Connection to PBX

Note: *if you configured the system with the Configuration Wizard then you can skip this step.*

The next step in the configuration is the connection to the PBX. This connection can be defined using the BCT System Settings. This central module is the web-based user interface to the United database used by BCT.

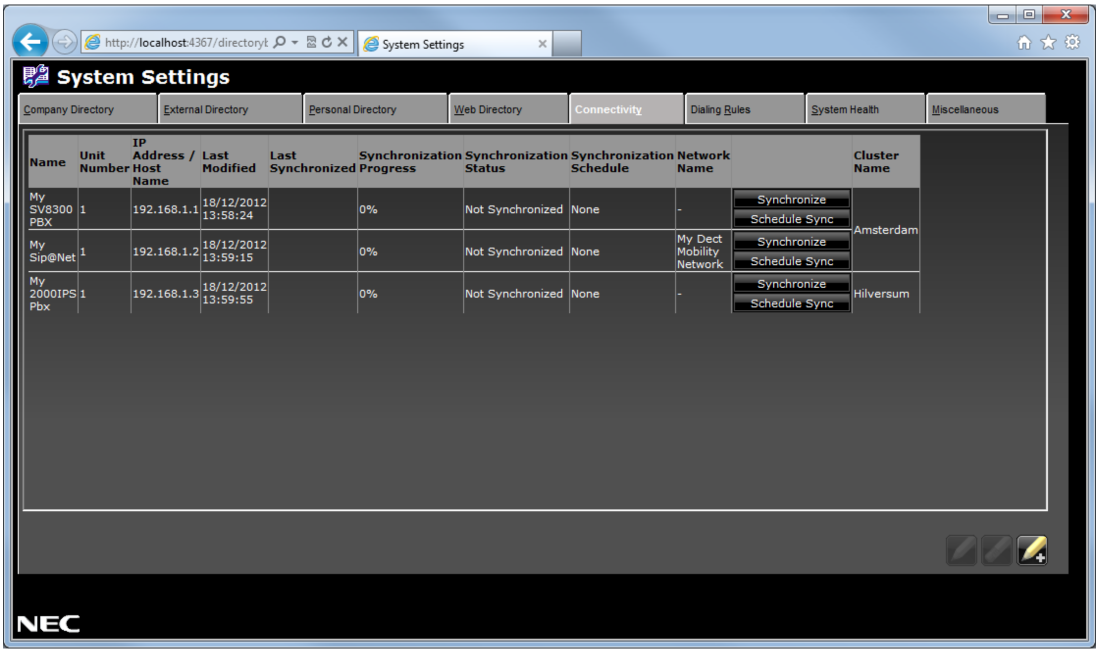
The administrator can login at: http://<servername>/ca/ca.aspx or select Start>Program files (x86)>Business ConneCT> BCT System Settings. Username: Administrator, no Password (default).

Note: *In case the BCT System Settings is started from a client PC in the domain, and your NT account is also listed with an employee role in the system, you might be immediately logged on in the system with employee rights. In that case, start the BCT System Settings from a client PC using the following URL: http://<servername>/ca/ca.aspx?wci=login Double click the shortcut two times since the first time, you will be again logged on with employee rights. The second time you'll get the BCT System Settings screen.*

Steps:

1. Login to BCT System Settings as **Administrator** (default no password). The first login from a new PC triggers a download of client components. Accept the download and press OK

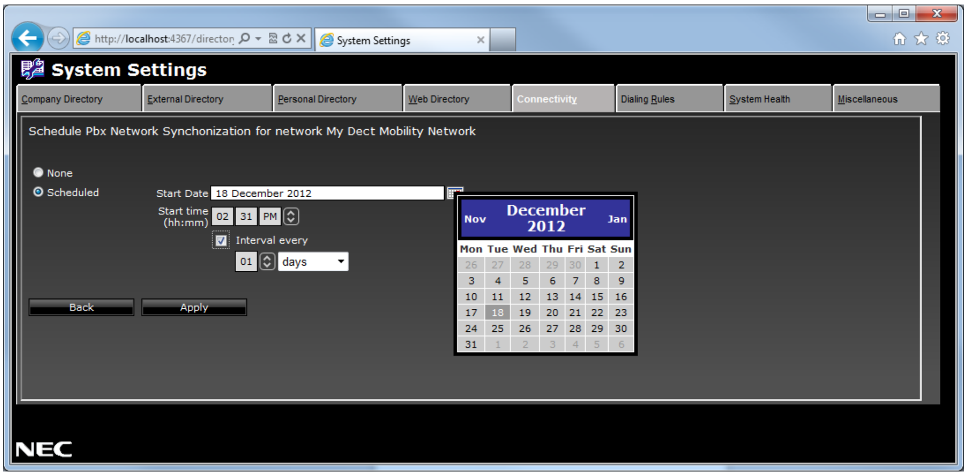
2. Select the **Connectivity** tab.



Name	Unit Number	IP Address / Host Name	Last Modified	Last Synchronized	Synchronization Progress	Synchronization Status	Synchronization Schedule	Network Name		Cluster Name
My SV8300 PBX	1	192.168.1.1	18/12/2012 13:58:24		0%	Not Synchronized	None	-	Synchronize Schedule Sync	Amsterdam
My Sip@Net	1	192.168.1.2	18/12/2012 13:59:15		0%	Not Synchronized	None	My Dect Mobility Network	Synchronize Schedule Sync	
My 2000IPS Pbx	1	192.168.1.3	18/12/2012 13:59:55		0%	Not Synchronized	None	-	Synchronize Schedule Sync	Hilversum

Figure 8-20 Connectivity Tab

3. **Schedule Sync**:
   If you press **Schedule Sync**, the set schedule synchronization page will appear:



Schedule Pbx Network Synchonization for network My Dect Mobility Network

○ None

● Scheduled

Start Date 18 December 2012

Start time (hh:mm) 02 31 PM

☑ Interval every

01 days

- If you select "None", no Synchronization is done, unless you request it manually.

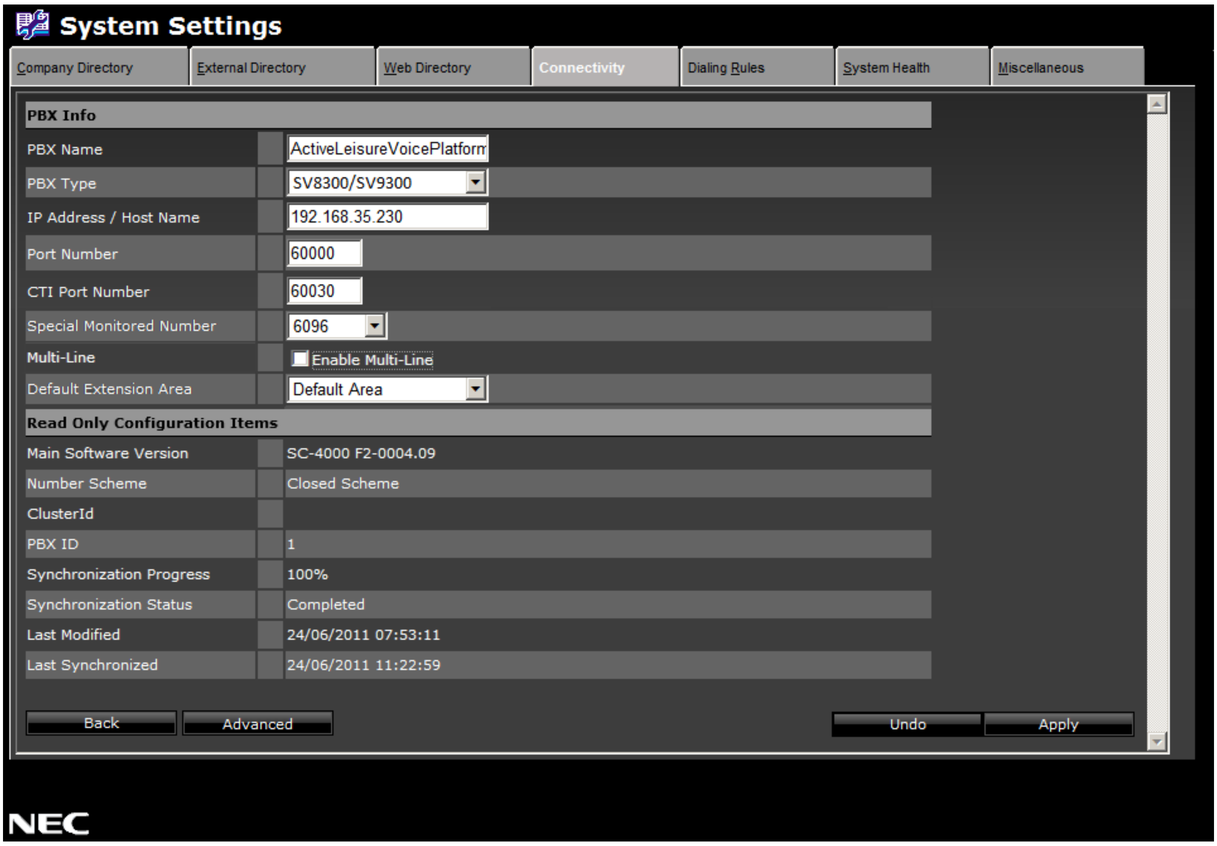
- If you select "Scheduled", specify date and time, and the repeating interval. It is advised to avoid unnecessary Synchronization, preferably outside office-hours.

Note: *In case you have an iS3000 IMP Network with several PBX units, you can use the synchronization as described above. Scheduling synchronization for one PBX will cause all PBXs in the network to be scheduled at the same time.*

4. Select the PBX and click the ‘Edit’ button (or click the 'Add' button to define a new one).

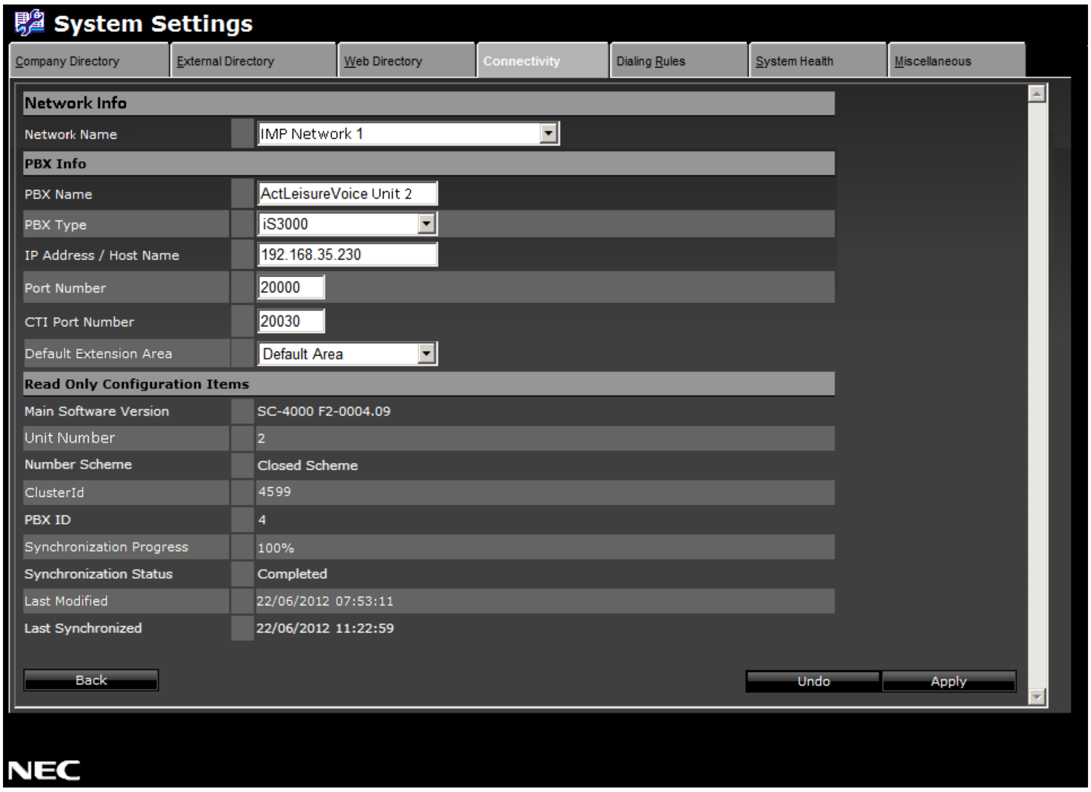
Note1: *Which items appear in this window, depends on the type of PBX.*

Note2: *In case your PBX type is iS3000, it is possible to connect to a multi-unit IMP Network. The Network name field will appear on top of the screen as an additional field, and PBX settings* *have to be specified for each PBX unit in the network. In this configuration BCT is aware of the PBX network, and not just of the individual PBXs.*



PBX Info	
PBX Name	ActiveLeisureVoicePlatform
PBX Type	SV8300/SV9300
IP Address / Host Name	192.168.35.230
Port Number	60000
CTI Port Number	60030
Special Monitored Number	6096
Multi-Line	□ Enable Multi-Line
Default Extension Area	Default Area
Read Only Configuration Items	
Main Software Version	SC-4000 F2-0004.09
Number Scheme	Closed Scheme
ClusterId	
PBX ID	1
Synchronization Progress	100%
Synchronization Status	Completed
Last Modified	24/06/2011 07:53:11
Last Synchronized	24/06/2011 11:22:59

Figure 8-21 Connectivity configuration – SV8300/SV9300 example



Network Info

Network Name	IMP Network 1

PBX Info

PBX Name	ActLeisureVoice Unit 2
PBX Type	iS3000
IP Address / Host Name	192.168.35.230
Port Number	20000
CTI Port Number	20030
Default Extension Area	Default Area

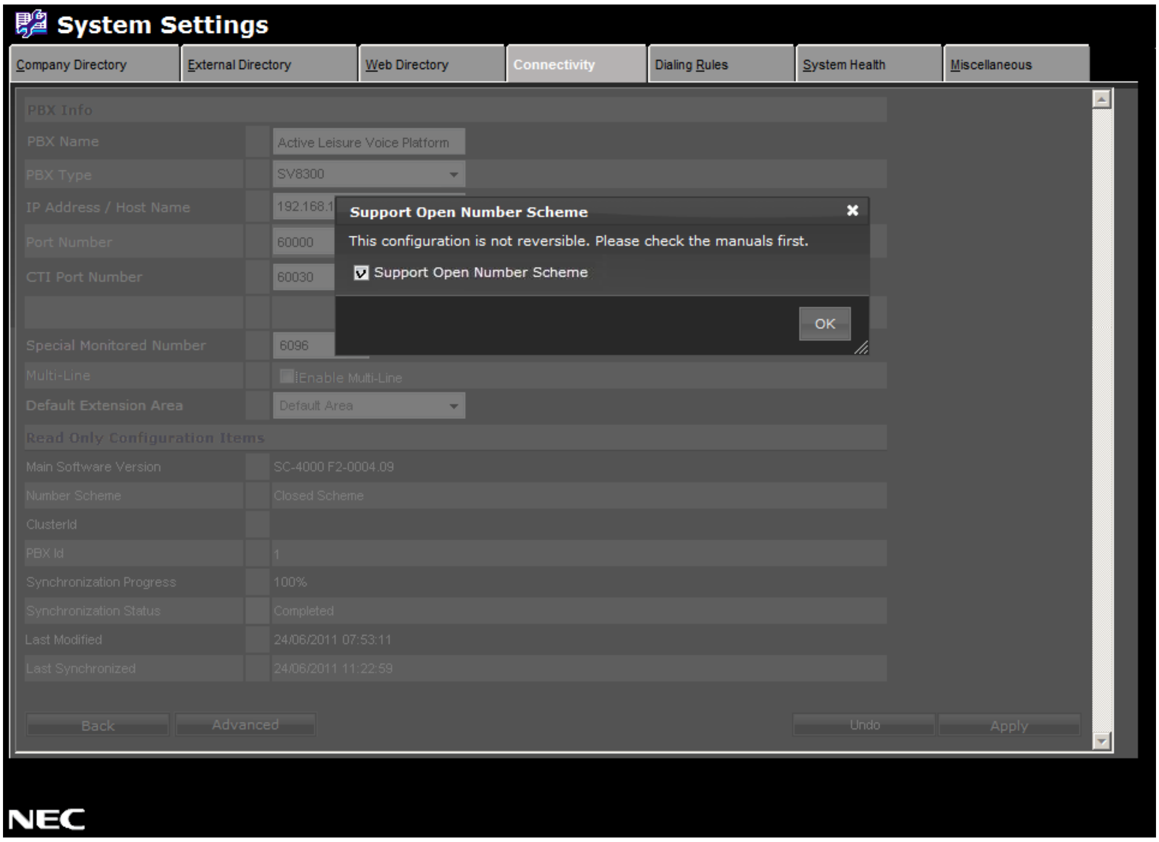
Read Only Configuration Items

Main Software Version	SC-4000 F2-0004.09
Unit Number	2
Number Scheme	Closed Scheme
ClusterId	4599
PBX ID	4
Synchronization Progress	100%
Synchronization Status	Completed
Last Modified	22/06/2012 07:53:11
Last Synchronized	22/06/2012 11:22:59

Figure 8-22 Connectivity configuration – iS3000 Network example

The **Advanced**-button is only visible if there is no PBX defined in the database - see Figure 8-21 Connectivity configuration – SV8300/SV9300 example. As soon as you have defined at least one PBX then the **Advanced**-button on the Added/Edit PBX Page is not visible anymore.

By default Closed Number Scheme is supported. Click on **Advanced**-button when Open Number Scheme must be supported (system-wide). A dialog window is shown:



PBX Info

PBX Name	Active Leisure Voice Platform
PBX Type	SV8300
IP Address / Host Name	192.168.1
Port Number	60000
CTI Port Number	60030
Special Monitored Number	6096
Multi-Line	□ Enable Multi-Line
Default Extension Area	Default Area

Read Only Configuration Items

Main Software Version	SC-4000 F2-0004.09
Number Scheme	Closed Scheme
ClusterId	
PBX Id	1
Synchronization Progress	100%
Synchronization Status	Completed
Last Modified	24/06/2011 07:53:11
Last Synchronized	24/06/2011 11:22:59

Support Open Number Scheme ✖

This configuration is not reversible. Please check the manuals first.

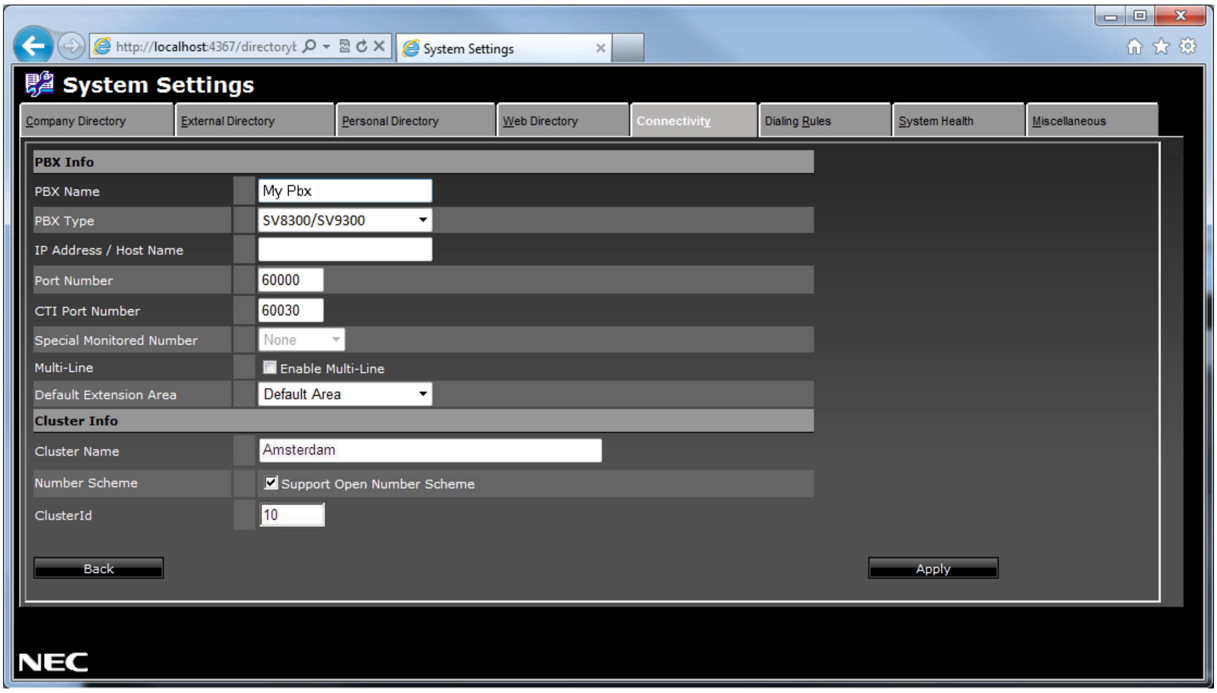
☑ Support Open Number Scheme

OK

Figure 8-23 Connectivity configuration – Open Number Scheme dialog box

The option you select defines whether this BCT installation shall support Open Number Scheme or not (System-wide). If not, no cluster specific info is required and will therefore not be visible in the edit PBX page (this is the default).

If you select Open Number Scheme and click on **OK** to return to the PBX / Edit page, then enter cluster information:



PBX Info	
PBX Name	My Pbx
PBX Type	SV8300/SV9300
IP Address / Host Name	
Port Number	60000
CTI Port Number	60030
Special Monitored Number	None
Multi-Line	□ Enable Multi-Line
Default Extension Area	Default Area
Cluster Info	
Cluster Name	Amsterdam
Number Scheme	☑ Support Open Number Scheme
ClusterId	10

Figure 8-24 Connectivity configuration – Open Number Scheme Cluster info

When adding an additional PBX, the user can assign the PBX to an existing cluster or can create a new cluster.

In case of creating a new cluster, and the PBX supports Open Number Scheme (only iS3000 and SV8300/SV9300 and SV9500 networks – not mixed), the user can select if the Cluster supports Open or Closed Number Scheme. In case Open Number Scheme is selected, the Cluster Name and Cluster Id/Office Number of this cluster can be entered. When the PBX does not support Open Number Scheme, the Cluster is automatically configured as closed and only the Cluster Name can be entered.

In case you want to assign the PBX to an existing Cluster you can select any existing cluster. Thus, when creating every additional PBX, it can be assigned to one of the existing clusters.

5. There are a number of other settings that need to be configured:

- Network Name: In case you have an iS3000 IMP Network: A name that clearly identifies the iS3000 IMP Network. You can add the PBX to an existing network or create a new network.

***Note**: You have to repeat configuring the settings for each PBX in the network. The unit numbers within the same network must be unique. Initially the unit numbers are not known (you cannot configure them yourself). They are retrieved during synchronization of the PBX. So synchronization will fail if the units within the network are not unique.*

- PBX Name: Any name that clearly defines this PBX
- PBX Type
- User Modification:

For UNIVERGE 3C there is an extra checkbox "User Modification". If checked, this will allow the information of Address Centric users to be overridden in BCT. By default this is switched off.

- IP address: IP address of the PBX
  - For an SV8500/SV9500 this is the address of the LAN2 (ACT) interface
  - for an iS3000 this is the IP address of the CPU card;
  - for an SV8100/SV9100 this is the IP address of the VoIP board;
  - for an AspireX/AspireUX this is the IP address of the VoIP board;
  - for an SV8300/SV9300 this is the IP address of the VoIP board;
    Note: if the IP address of the PBX is related to a Host name then this Host name is also allowed.
  - for a UNIVERGE 3C this is the IP address of the UNIVERGE 3C Manager
- Name Synchronization:
  For SV8100/SV9100 there is an extra checkbox "Name synchronization". By default this is switched on. During Synchronization the extension names in the SV8100/SV9100 will be inserted as users into the Company Directory of BCT (only if the name was not yet filled in).

- Default Extension Area: Your system may have one Default Area or several areas for dialing rules (see 8.1.1 Using the Configuration Wizard and 18 Appendix H – DIALING RULES AND NUMBER CONVERSION). Select the area applicable for this PBX.
  All extensions created after this, will automatically be related to the selected area.

- Special Monitored number must be programmed in the PBX (see relevant PBX chapter).
  Note: during the creation of the PBX no numbers are known. To fill in the Special Monitored number, leave this number empty during creation and after Synchronization of the PBX edit this number from the drop-down list.

- Location Name (iS3000 / SV8300/SV9300 / SV8500/SV9500 / UNIVERGE 3C / SV9100-TAPI): Select the location name as defined for the Call Recording Location.

- PBX UserName (SV8100/SV9100 / AspireX/AspireUX, SV8500/SV9500, UNIVERGE 3C)
  Note: A UNIVERGE 3C user must have Domain User rights.

- PBX Password (SV8100/SV9100 AspireX/AspireUX, SV8500/SV9500, UNIVERGE 3C)

- Call Forwarding Settings (SV8300/SV9300 / SV8500/SV9500); you can enable Split call forwarding, to make a distinction between internal calls and external calls. Must be available in PBX.

- Zone selection: (UNIVERGE 3C only)
  In the UNIVERGE 3C zones can be defined (See 4.6.4.9 Configure CTIuser and 4.6.4.13 Configuring Open Numbering Plan).
  - UNIVERGE 3C server has (by default) Open Numbering Plan not enabled
    Do **NOT** check checkbox “3C System has Open Numbering Plan enabled”.
    With ZoneSync button, zones are retrieved from the UNIVERGE 3C and shown in a table above the ZoneSync button. For a zone, the company or external directory can

be selected. On Apply and synchronize the company and external directory are updated accordingly.

- UNIVERGE 3C server has Open Numbering Plan enabled
  Check checkbox "3C System has Open Numbering Plan enabled".
  When the PBX is initially created and the Apply button is clicked, the zones of the CTIUser are retrieved from the PBX and shown in the edit page.
  Normally only one zone will be shown but if there are more, select the zone(s) to be included as company zone.
  Note down the ZoneId shown in the most right column of the zone list, this integer value is needed when creating the stations for VMP lines and Routing Points using the 4.6.3 UNIVERGE 3C SIP Line Configurator.
  Before continueing synchronizing the PBX, create the VMP and Routing point stations with 4.6.3 UNIVERGE 3C SIP Line Configurator (do **not** forget to check the "Open Numbering Plan" and fill in the value of ZoneId) and assign them to the related addresses in UNIVERGE 3C administrator in the zone selected from the zone list.
  On Apply and synchronize the company directory is updated accordingly.

6. Select "Apply" to save the settings.

WARNING: *You must synchronize (either manually or automatically) after you make changes to a PBX.*

Synchronization may take time and claim a lot of resources. IF the system is low on memory, YOU SHOULD synchronize individual PBXs MANUALLY. In all cases be patient with the system.

IF there are more PBXs, then it is advised not to synchronize them in parallel, but schedule them with different time intervals.

Note*: In case you have an iS3000 IMP Network with several PBX units, and you synchronize manually, there will be only one Synchronize button per network. All units in the network must be synchronized at the same time.*

Note*: There is a special feature to synchronize PBXs after you moved extensions to another PBX. Details can be found in 31 Appendix U – Move extensions to other PBX*

8.1.6. Start and configure the BCT Platform

The Contact Center part of BCT is based on the BCT platform. The user interface of this platform consists of two applications:

- BCT Supervisor Dashboard: the user interface to create call-flows etc.
- Runtime Manager: the background application controlling all events.

To start BCT, you must also start UCS Runtime, so users can log in, section 8.1.7 UCS Runtime . The Runtime manager cannot start before the application is connected to the database.

To configure or make changes to an already configured BCT application, you must use the BCT Supervisor Dashboard.

***Note:** You can only start the BCT configuration after the database is created. For operator related routing, such as Queues, you must restart the operator client.*

1. To start the BCT Supervisor Dashboard, go to **Start > Programs > Business ConneCT > Business ConneCT Supervisor Dashboard**, or start the Business ConneCT Supervisor Dashboard application from the application tiles. You are asked to login.

A predefined user account is available for administrator tasks. The logon name is "Administrator". Initially the password is empty. Click OK.

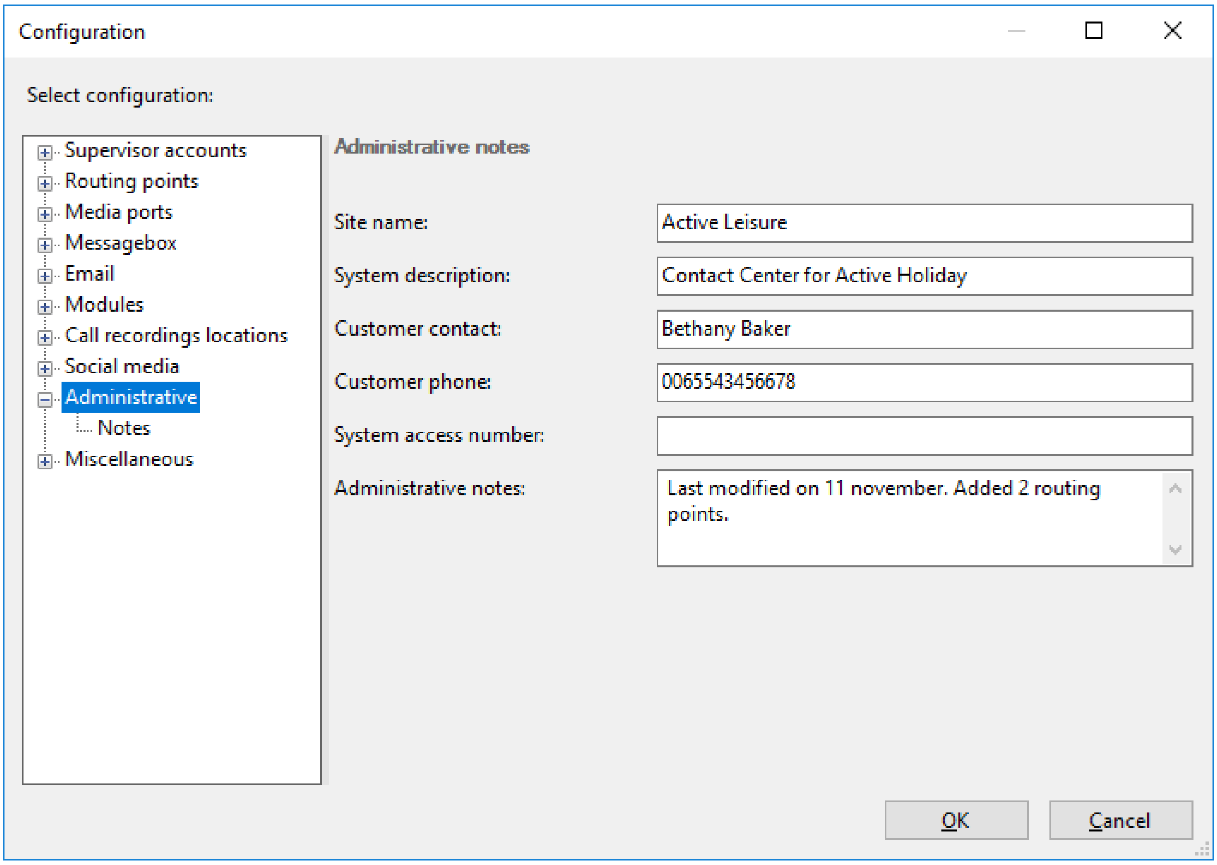
The password can be changed for better security. Select **Change Password** from the **Tools** menu.

2. Select **Configuration** from the **Tools** menu. The configuration window is displayed. The items of this window are described in the following subsections.

***Note:** Some items can also be configured using the Configuration Wizard. You can use this wizard for simple configurations, e.g. one PBX. If the configuration is more complex, then use the BCT Supervisor Dashboard.*

8.1.6.1. Administrative Notes

The "Administrative - Notes" item allows you to enter useful information about the customer, the site etc. This is a good location to store contact information and important system information.



Site name: Active Leisure

System description: Contact Center for Active Holiday

Customer contact: Bethany Baker

Customer phone: 0065543456678

System access number:

Administrative notes: Last modified on 11 november. Added 2 routing points.

Figure 8-25 BCT Supervisor Dashboard - Configuration, Administrative Notes

Examples of important information are: software versions of BCT and the PBX, how to reach the customer, the name of the used database and the History of the site.

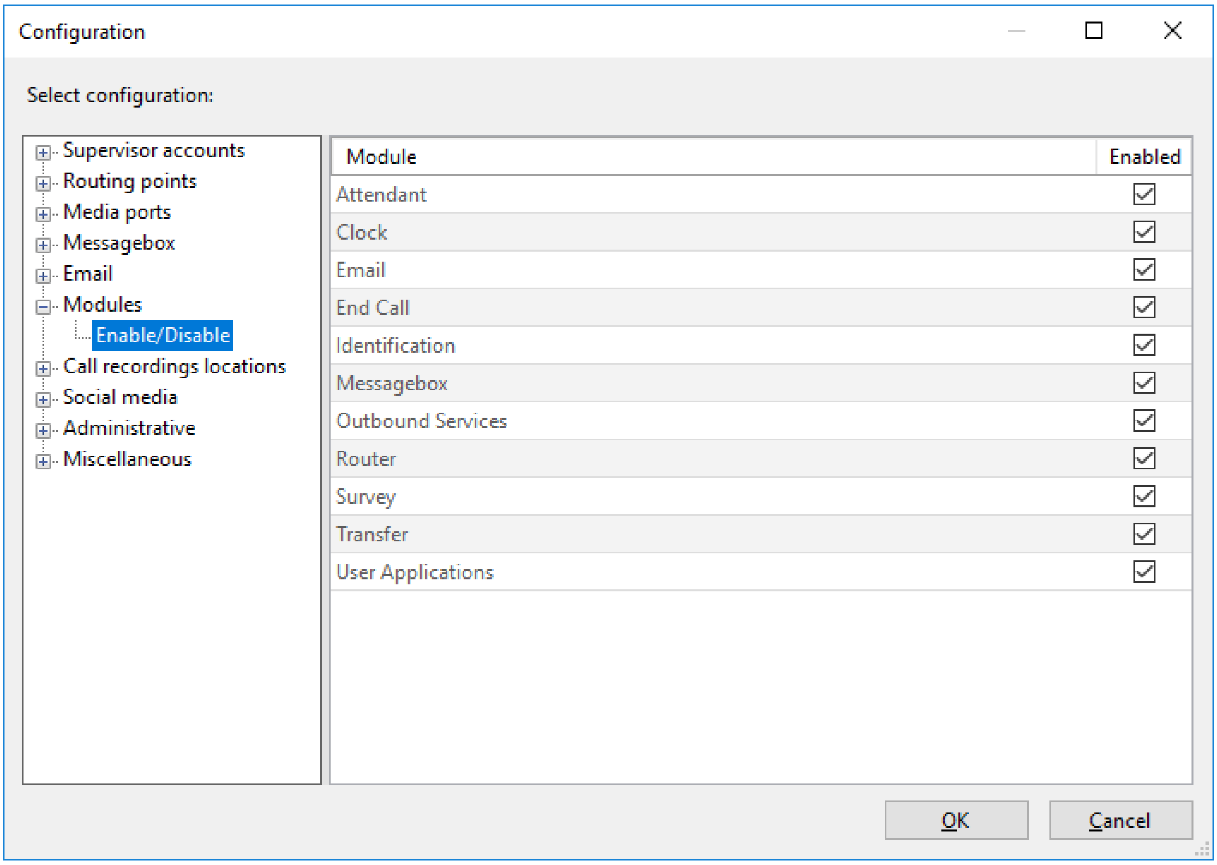
8.1.6.2. Languages

See section 8.1.12 Miscellaneous point 1.

8.1.6.3. Modules

The BCT Supervisor Dashboard can enable or disable modules. Examples are: Router, Clock, Email etc. Select “Modules - Enable/Disable” and mark the check box (Enabled) for only those modules relevant for this system. A complete explanation about these modules can be found in the BCT Administrator Guide.

The changes that you are making for the Modules are only displayed after the configuration data is saved by clicking the **OK** button.

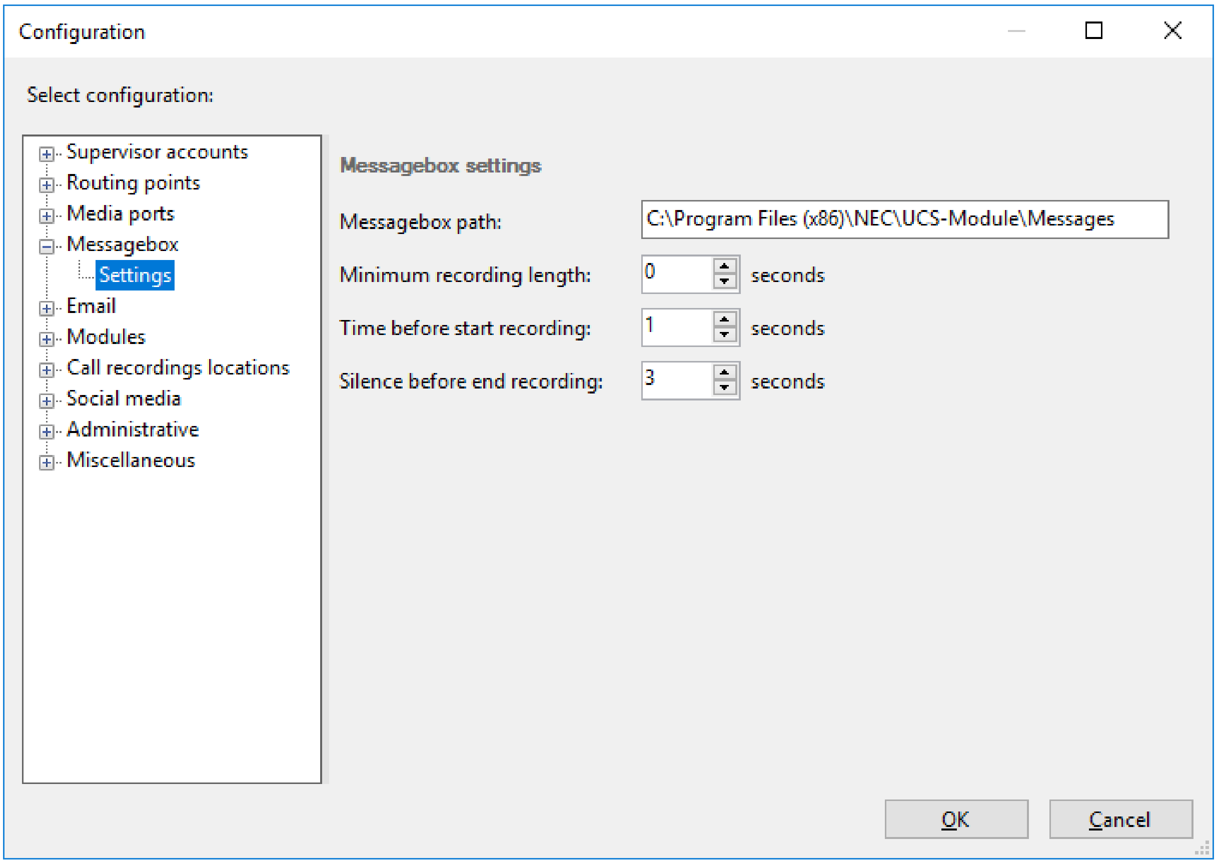


Module	Enabled
Attendant	☑
Clock	☑
Email	☑
End Call	☑
Identification	☑
Messagebox	☑
Outbound Services	☑
Router	☑
Survey	☑
Transfer	☑
User Applications	☑

Figure 8-26 **BCT Supervisor Dashboard** - Configuration, Modules

8.1.6.4. Messagebox Settings

The “Messagebox - Settings” item contains the main directory for stored messages and recorded announcements and recorded calls.



Messagebox settings

Messagebox path: C:\Program Files (x86)\NEC\UCS-Module\Messages

Minimum recording length: 0 seconds

Time before start recording: 1 seconds

Silence before end recording: 3 seconds

Figure 8-27 BCT Supervisor Dashboard - Configuration, Messagebox settings

- **Messagebox path**
  Enter the directory on the BCT server that will be used for messages.

  The entered directory is the main directory. The system will create subdirectories for each messagebox that is created. This subdirectory will contain three other subdirectories, one for voice messages, one for recorded announcements and one for call recordings made by a user.

  Note: *When changes to the Messagebox Path are made, the next steps must be performed:*
  - Copy all information (all subdirectories and web.config file) to the new location.
  - In IIS change the MessageBoxes (under tree-item Sites, Default Web Site) configuration.
  - Select MessagBoxes and via Advanced Settings, change the Physical path to the new location.
  - Reboot the server to take effect of the change.

  After an upgrade, make sure that the MessageBox setting in IIS is still the new location.

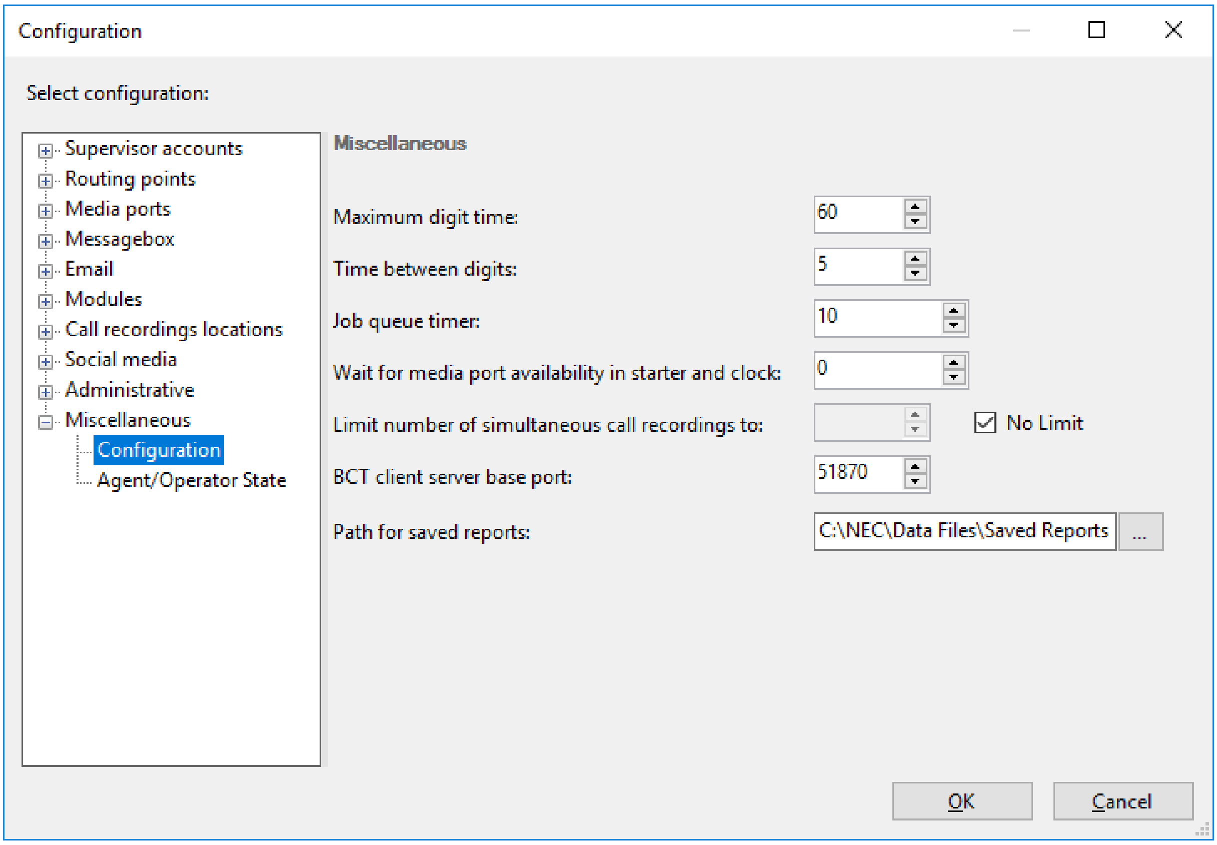
- **Minimum recording length**
  The minimum length of a recorded message, this to avoid empty messages, a normal value would be 3 seconds.

- **Time before start recording**
  This is the time between the message (e.g. "... *leave your name and number after the tone*") and the actual tone.

- **Silence before end recording**
  This is the time after which the system will disconnect when receiving silence.

8.1.6.5. Miscellaneous Configuration

The "Miscellaneous - Configuration" item contains the default settings for the voicemail system (if integrated Voicemail is used – see 8.1.12 Miscellaneous) and some more general settings.



Maximum digit time: 60

Time between digits: 5

Job queue timer: 10

Wait for media port availability in starter and clock: 0

Limit number of simultaneous call recordings to: ☑ No Limit

BCT client server base port: 51870

Path for saved reports: C:\NEC\Data Files\Saved Reports ...

Figure 8-28 **BCT Supervisor Dashboard** - Configuration, Miscellaneous, Configuration

- **Maximum digit time**
  The maximum time the system waits for the user to enter a range of digits.

- **Time between digits**
  A caller must press the next digit before the defined time expires.

- **Job queue timer**
  Scan period for outbound jobs.

- **Wait for Media Port availability in Starter and Clock (sec)**
  The waiting period for prompts defined in Starter and Clock. When the call flow reaches the first greeting from these two modules, it will wait to get a VMP line for as long as the time specified. When waiting expires, the call flow will proceed.

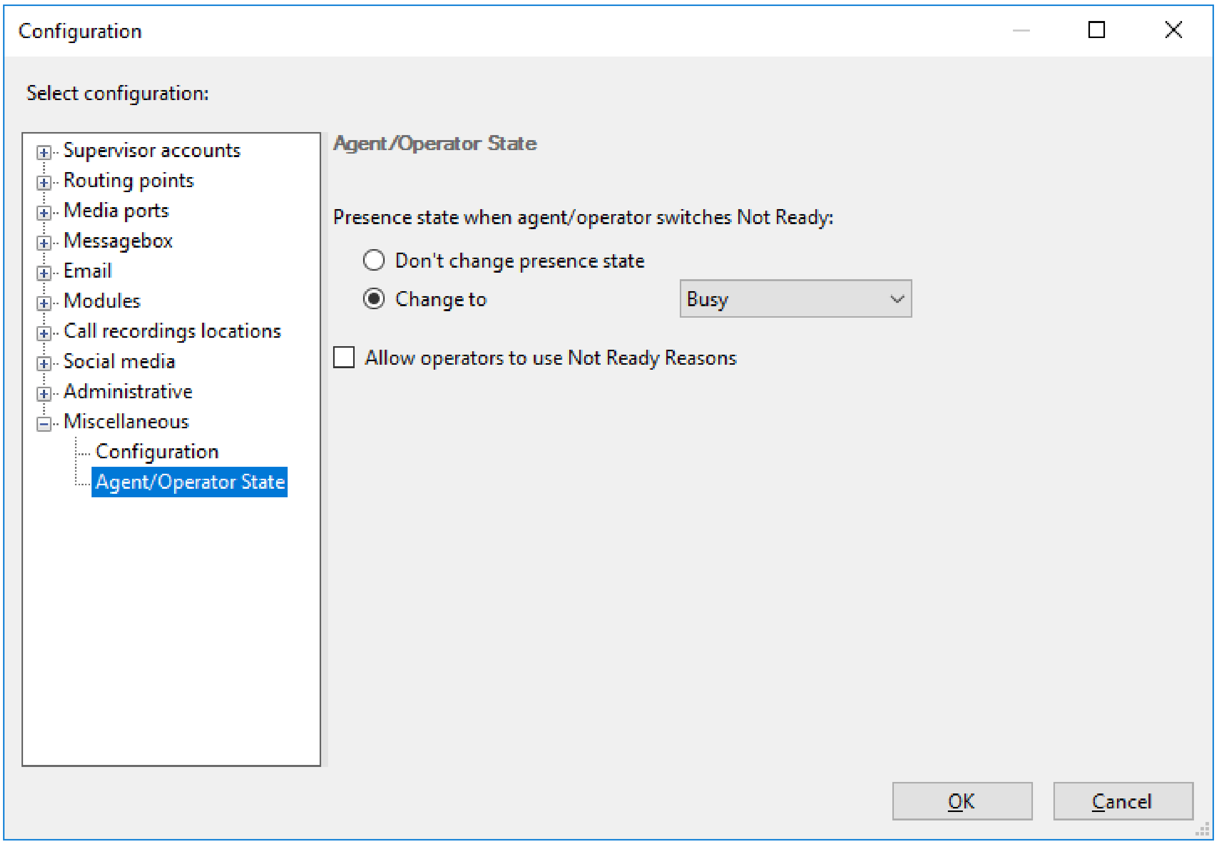
- **Limit number of simultaneous call recordings to**
  The maximum number of call recordings by users that can be run simultaneously. When the maximum number has reached then other users (operator, agent, employee) will not be able to start call recording. Click the "No Limit" checkbox if no limitation is needed. Number of simultaneous call recordings can then grow up till the number of configured (and available) media ports.
  Note: when all media ports are in use by call recording then no line will be available anymore for interactive voice response.

- **BCT client server base port**
  The base-port is used for Client/Server communication.
  Only available when the BCT Supervisor Dashboard runs on the BCT server.

- **Path for saved reports**
  The folder on the server machine where scheduled reports are saved when ouput is set to “Save to disk”. The browse button is available when the BCT Supervisor Dashboard runs on the BCT server.

8.1.6.6. Agent/Operator State

The “Miscellaneous – Agent/Operator State” item contains settings that are related to the agent and/or operator state.



Agent/Operator State

Presence state when agent/operator switches Not Ready:

○ Don't change presence state

● Change to Busy

□ Allow operators to use Not Ready Reasons

Figure 8-29 **BCT Supervisor Dashboard** - Configuration, Miscellaneous, Agent/Operator State

- **Presence state when agent switches Not Ready**
  By default when an agent switches Not Ready his presence state won’t change. If that should change along with setting Not Ready then select a presence state from the drop down box. The agent’s presence will automatically switch back to Online when agent switches Ready again.

- **Allow operators to use Not Ready Reasons**
  By default operators can take a break by using the “Coffee break” button. When this option is set then operator can specify the reason of the break by selecting one of the pre-defined Not Ready Reasons.

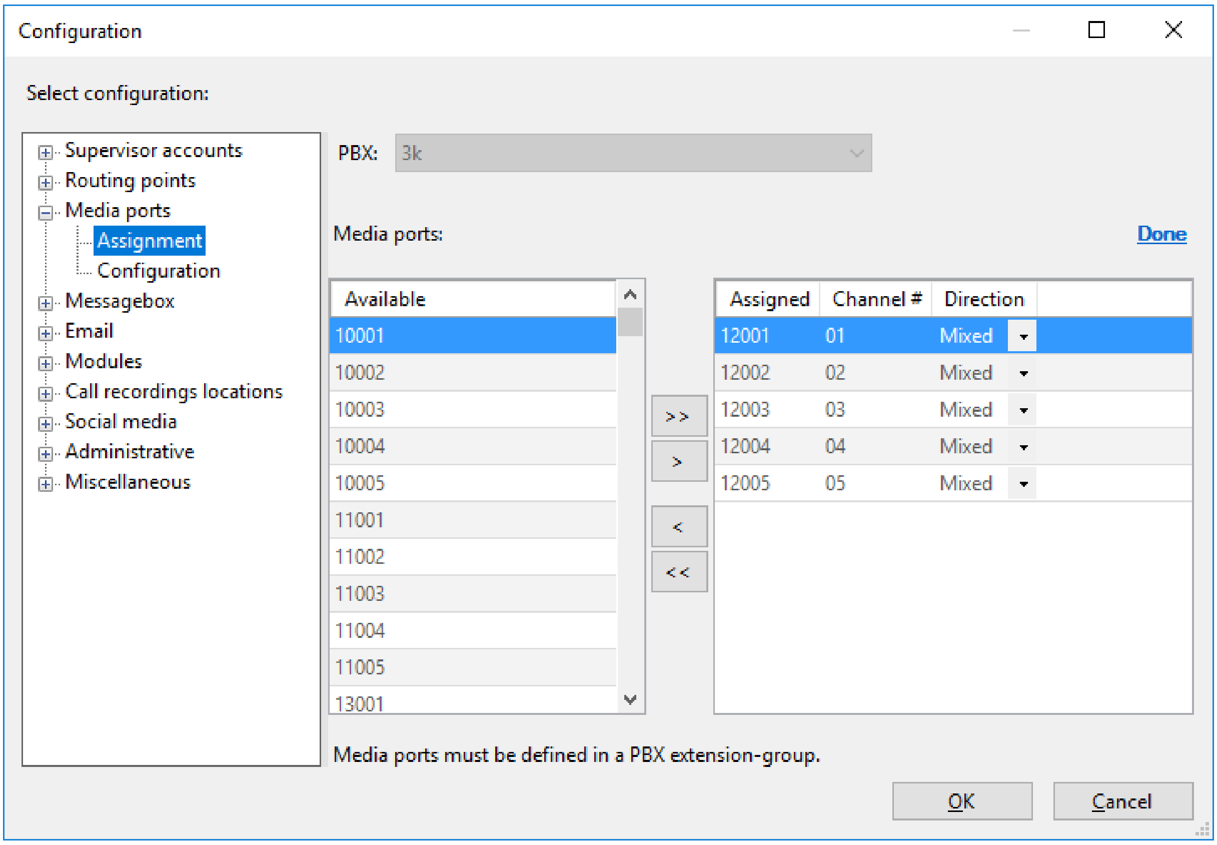
8.1.6.7. Media Ports Assignment

Note: *If you have configured the system using the Configuration Wizard, you can skip this section.*

1. Go to the “Media Ports - Assignment” item.

2. If you have multiple PBXs, you must select one. The system will only offer suitable lines from that PBX.

In this screen you need to fill in line properties of the lines between the VMP software and the PBX. These are NOT the agent extensions!



PBX: 3k

Media ports: Done

Available
10001
10002
10003
10004
10005
11001
11002
11003
11004
11005
13001

Assigned	Channel #	Direction
12001	01	Mixed
12002	02	Mixed
12003	03	Mixed
12004	04	Mixed
12005	05	Mixed

Media ports must be defined in a PBX extension-group.

Figure 8-30 BCT Supervisor Dashboard - Configuration, Media Ports Assignment

3. Click on ‘Add/Remove’ to change the assignment of media ports.

4. Click ‘Done’ to go back to list of assigned media ports.

5. Enter the channel number and select the direction (whether it is used for inbound or outbound traffic, or mixed) in the grid.

After programming new lines in the PBX, these lines are not automatically visible in the ‘Available lines’ window. To fix this, synchronize the PBX using the BCT System Settings, see section 8.1.5 Connection to PBX.

8.1.6.7.1. Media Ports Configuration on SV9100-TAPI for Voice Mail

In addition to the above section:
Within SV9100 it is possible to assign a Voice Mail Department Group with program command 45-01-01. By default the number assigned here is 64 (the internal Voice Mail system of SV9100) redirecting a call to the voice mail of the destination when an internal initiator presses the “VMsg” softkey while calling or uses quick access.
When assigned another group with standard SIP members, BCT voice mail can be used instead of the internal SV9100 voice mail system.

The members of this department group are also shown in the Available Media ports however with an asterisk to indicate that these lines are member of the voice mail group, where (de)assigning (move between left and right pane) is equal to 'normal' VMP lines but indicated with an asterisk.
To have correct operation program command 45-01-02 shall be set to "Sending DTMF Tone to SLT-VM port".

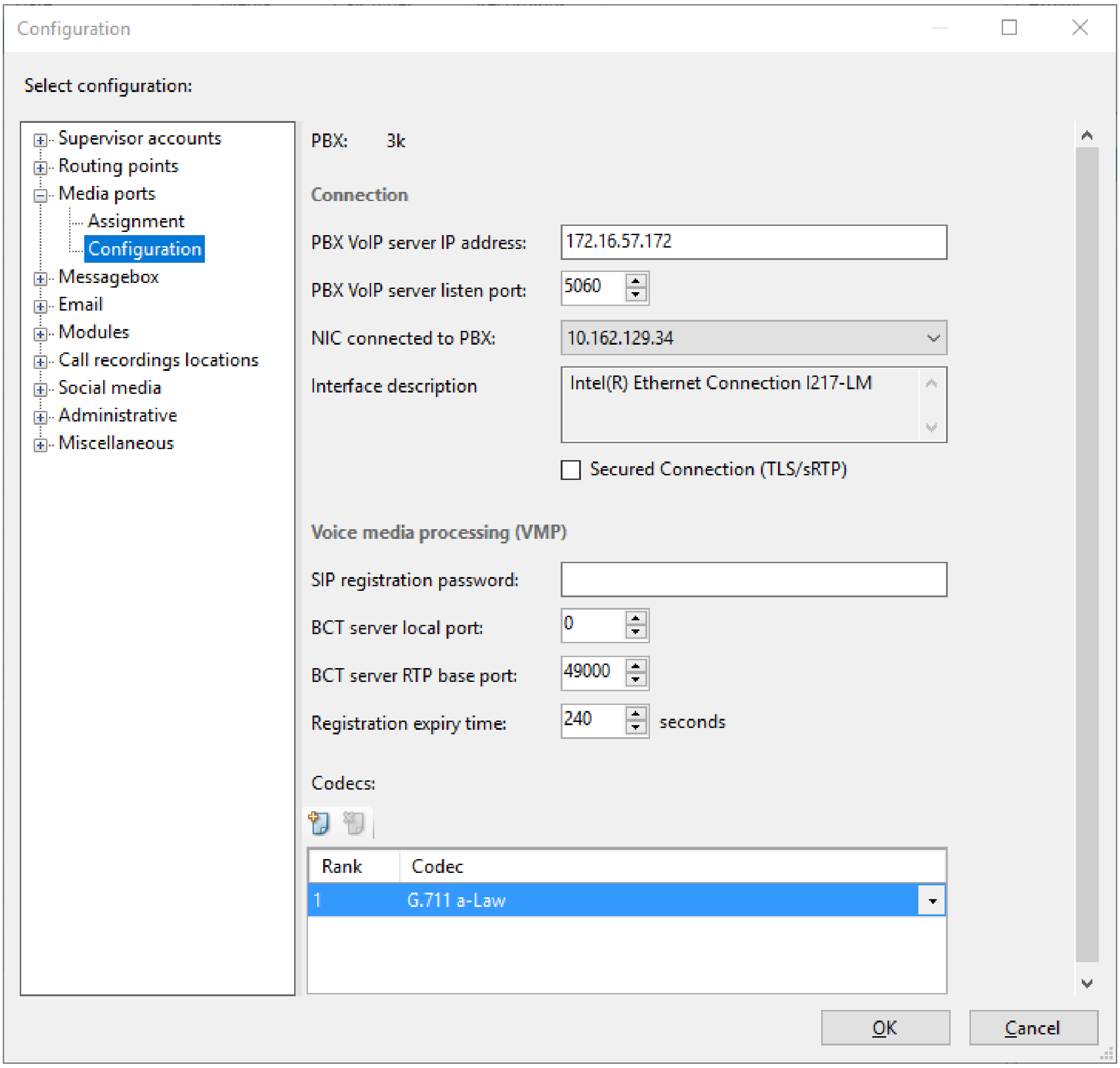
Notes:

- VMP lines marked with an asterisk can **only** be used for incoming voice mail and will have direction "Inbound" only
- The starter for messagebox access shall **NOT** be the pilot number of the voice mail group; use the pilot number of the 'normal' VMP lines instead or use one of the not assigned routing points
- The VMP lines with an asterisk are counted on licenses like 'normal' VMP lines.

8.1.6.8. Media Ports Configuration

Note: *If you have configured the system using the Configuration Wizard, you may skip this section.*

1. Go to the "Media Ports - Configuraton" item. If no VMP lines have been defined, then this tab will not be shown. There are two versions of this, depending on whether it runs on the server or on a client machine.
2. Depending on the used PBX-type, the Media Ports are SIP-based or IP-Protims based. SIP is used by SV8100/9100, AspireX/AspireUX, iS3000 and UNIVERGE 3C PBX. IP-Protims (DRS) is used by SV8300/9300 and SV8500/9500 PBX.



PBX: 3k

Connection

PBX VoIP server IP address: 172.16.57.172

PBX VoIP server listen port: 5060

NIC connected to PBX: 10.162.129.34

Interface description: Intel(R) Ethernet Connection I217-LM

□ Secured Connection (TLS/sRTP)

Voice media processing (VMP)

SIP registration password:

BCT server local port: 0

BCT server RTP base port: 49000

Registration expiry time: 240 seconds

Codecs:

Rank	Codec
1	G.711 a-Law

Figure 8-31 BCT Supervisor Dashboard - Configuration, Media Ports Configuration

- **Connection**
  Enter the IP address and port of the VoIP card (SV8100/SV9100 / AspireX/AspireUX) or SIP-Server (iS3000 and UNIVERGE 3C) that provides the VoIP service. The default port is predefined based upon selected PBX-type. The port can be adapted when required (e.g. because the SIP-service on PBX has been configured to non-default port), but usually this is not changed in the PBX.

  Secured SIP + Media (TLS+sRTP) can be applied for SIP-based media [currently only supported for UNIVERGE 3C and SIP@Net]. To enable this, check the Secure Media checkbox.

  The "Interface"-field (NIC) is the IP address used by the runtime to interface towards the PDS-Server or to the SIP-Server. This field is not visible on a client (BCT Supervisor Dashboard) machine.
  If on the server-machine there is only one network-card (with only one IP address), then this IP address is selected by default and the combo box is disabled.

  - **Voice Media Processing (VMP)**
    You can enter a password for secured SIP Digest Authentication. This applies only for SIP based connections and will be used when the SIP-server enforces Digest Authentication.

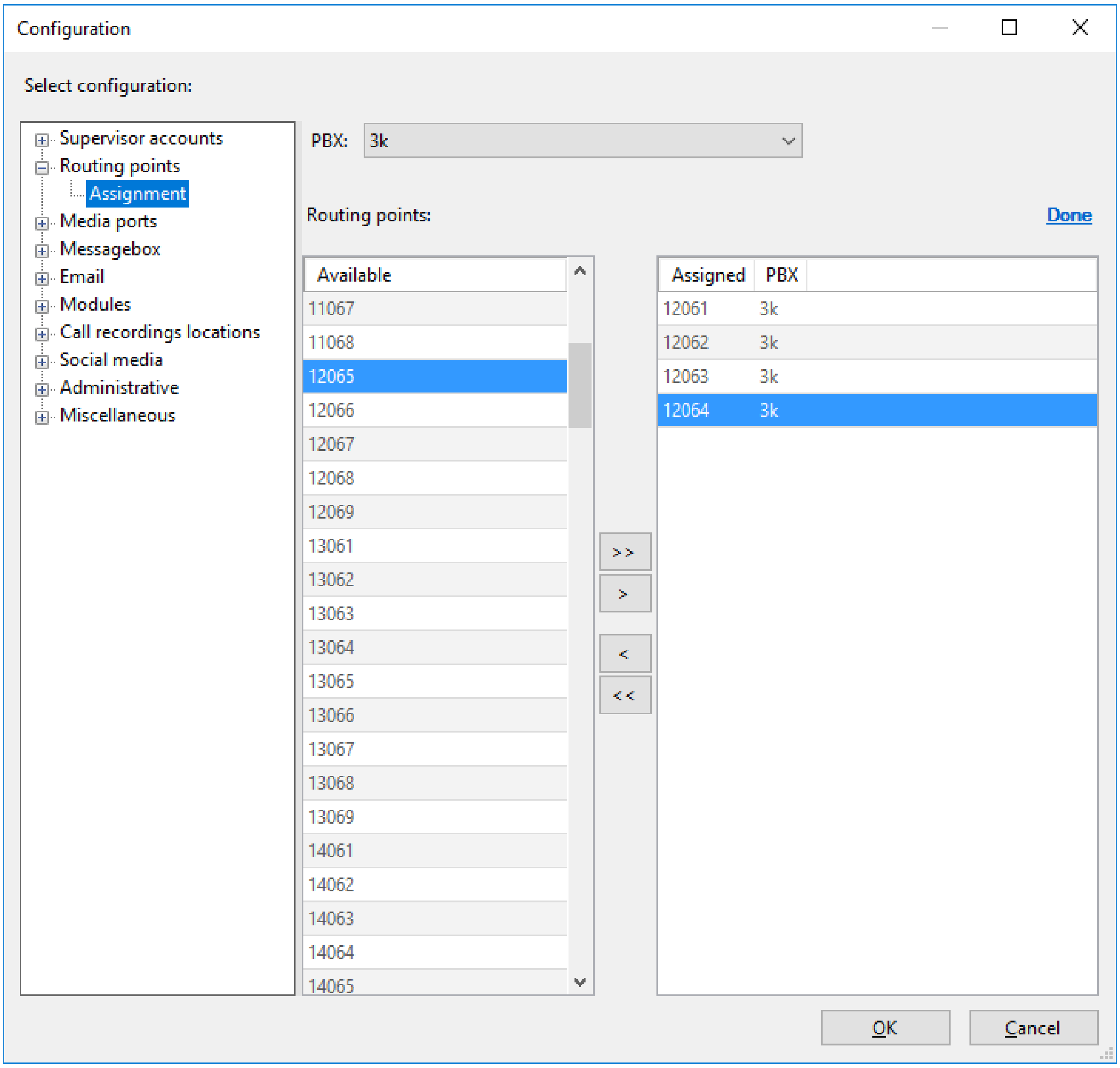
UNIVERGE 3C does not support SIP Digest Authentication.
The “Registration Expiry Time” applies only to SIP and specifies how often you want the media lines re-register with the PBX.
For the ports, enter the appropriate port numbers (the defaults are recommended). “Server Local Port” (for signaling) value 0 means that the port is assigned dynamically by Windows OS. Using value 0 for “RTP Base Port” is not recommended.

- **Codec Data**
  For Codec Data, the recommended settings are G.711 a-Law or G.711 µ-Law codec (depending on localization). These offer the best audio quality.
  G.729 is also available, but uses lower bandwidth by higher compression and so less quality.

8.1.6.9. Routing Points

1. Go to the “Routing Points - Assignment” item.

2. Click on ‘Add/Remove’ to change the assignment of routing points. Click ‘Done’ to go back to list of assigned routing points.



PBX: 3k

Available
11067
11068
12065
12066
12067
12068
12069
13061
13062
13063
13064
13065
13066
13067
13068
13069
14061
14062
14063
14064
14065

Assigned	PBX
12061	3k
12062	3k
12063	3k
12064	3k

Figure 8-32 **BCT Supervisor Dashboard** - Configuration, Routing points

3. If you have multiple PBXs, select one to view only routing points in that PBX, otherwise all routing points are shown.

In IVR less configurations you must assign Routing Points so the system to know what the Monitored numbers are.

- For SV8300/SV9300 and SV8500/SV9500, these are the OAI Monitored numbers.
- For iS3000 the Routing Points are ACD groups.
- For SV8100/SV9100 / AspireX/AspireUX the Routing Points are department groups with Virtual Extension members.

If the numbers are not visible, synchronize the BCT Server with the PBX data. See 8.1.5 Connection to PBX. Assign the Routing Point by selecting the line from the available list and move it to the assigned list with the arrow, in this case the order is not important.

8.1.6.10. Email Servers

Refer to the BCT Administrator Guide chapter “Create an Email server”.

8.1.6.11. Email Rules

You can define some general rules for Email handling.

Refer to the BCT Administrator Guide chapter “Creating Email rules”.

You can define these rules during initial installation or in a later phase.

8.1.6.12. Call recording locations

Refer to the BCT Administrator Guide chapter “Call recording”.

8.1.6.13. Social media providers

Refer to the BCT Administrator Guide chapter “Create a Social Media provider”.

8.1.6.14. Social media attachments

Refer to the BCT Administrator Guide chapter “Configure Social media Attachments”.

8.1.7. UCS Runtime

After the system is configured, open the Runtime Manager via **Start > Programs > Business ConneCT > Tools > Runtime Manager**. Press **Start System** to start.

Important: *By default the UCS Runtime has to be started manually after every reboot, this can also be set as an automatic service via Start > Control Panel > Administrative tools > Services. Right-click the* ***NEC Unified Contact Server*** *service and select properties. Set the start-up type to automatic and press OK.*

8.1.8. Selective Monitoring

You can exclude numbers from monitoring. This will improve the startup time. If you want to monitor only those extensions that have a related BCT user, execute the following steps.

1. Open the Configuration Manager and select the configuration file: “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config”.

2. Locate the key: SeatMonitorLevel

3. Change value to “1”

4. Press button Save to store the value.

5. Restart UCS Runtime service.

The SeatMonitorLevel key can have the following values:

- 0: monitor all existing seats by the startup of the application.
- 1: monitor only the extensions of users with a client role and the phone based agents.
- 2: monitor all the created users (this is the default value).

Note: *The UCS Runtime has to be restarted.*

8.1.9. Voicemail configuration

Note: *If you have configured the system using the Configuration Wizard, you can skip this chapter.*

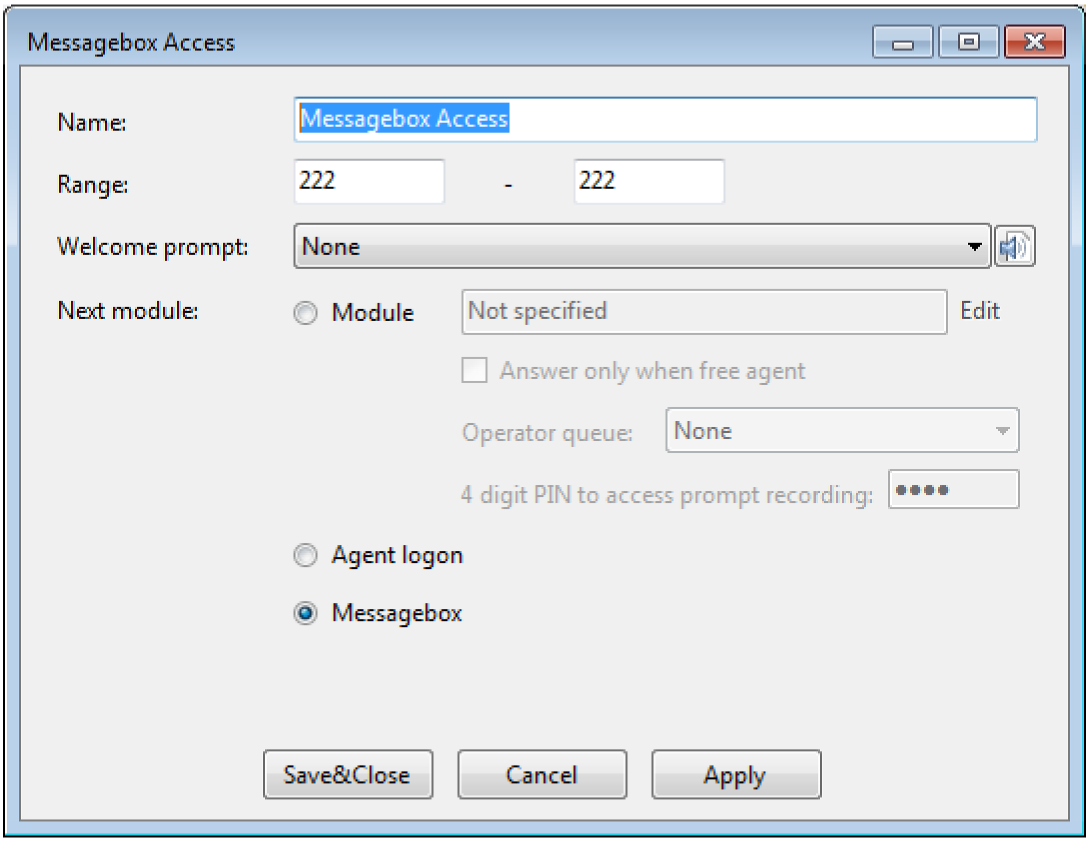
Note: *Applies to Integrated Voicemail only – See 8.1.12 Miscellaneous for external Voicemail.*

Voicemail configuration relies on two major steps: creation of the message boxes and distributing access right of these message boxes to the users. The message boxes are created automatically, access rights are distributed via the Central Authentication module.

The voicemail application uses the same configuration in the PBX as the Contact Center. A special access number must be programmed for voicemail access pointing to the Routing Point. Be sure the correct (country dependent) tone-plan is loaded in the PBX, since the voicemail uses DTMF tones.

1. Login to the BCT Supervisor Dashboard

2. Create a new Starter Line. This Starter Line points to the access number dedicated for voicemail. Enter the properties according to the following figure:



Messagebox Access

Name: Messagebox Access

Range: 222 - 222

Welcome prompt: None

Next module: ○ Module Not specified Edit

□ Answer only when free agent

Operator queue: None

4 digit PIN to access prompt recording: ••••

○ Agent logon

● Messagebox

Figure 8-33 Properties of the voicemail starter line, in this example 222 is the access number for voicemail.

3. Make sure the VMP lines are correctly connected to VMP ports see BCT Supervisor Dashboard and section: 8.1.6.7 Media Ports

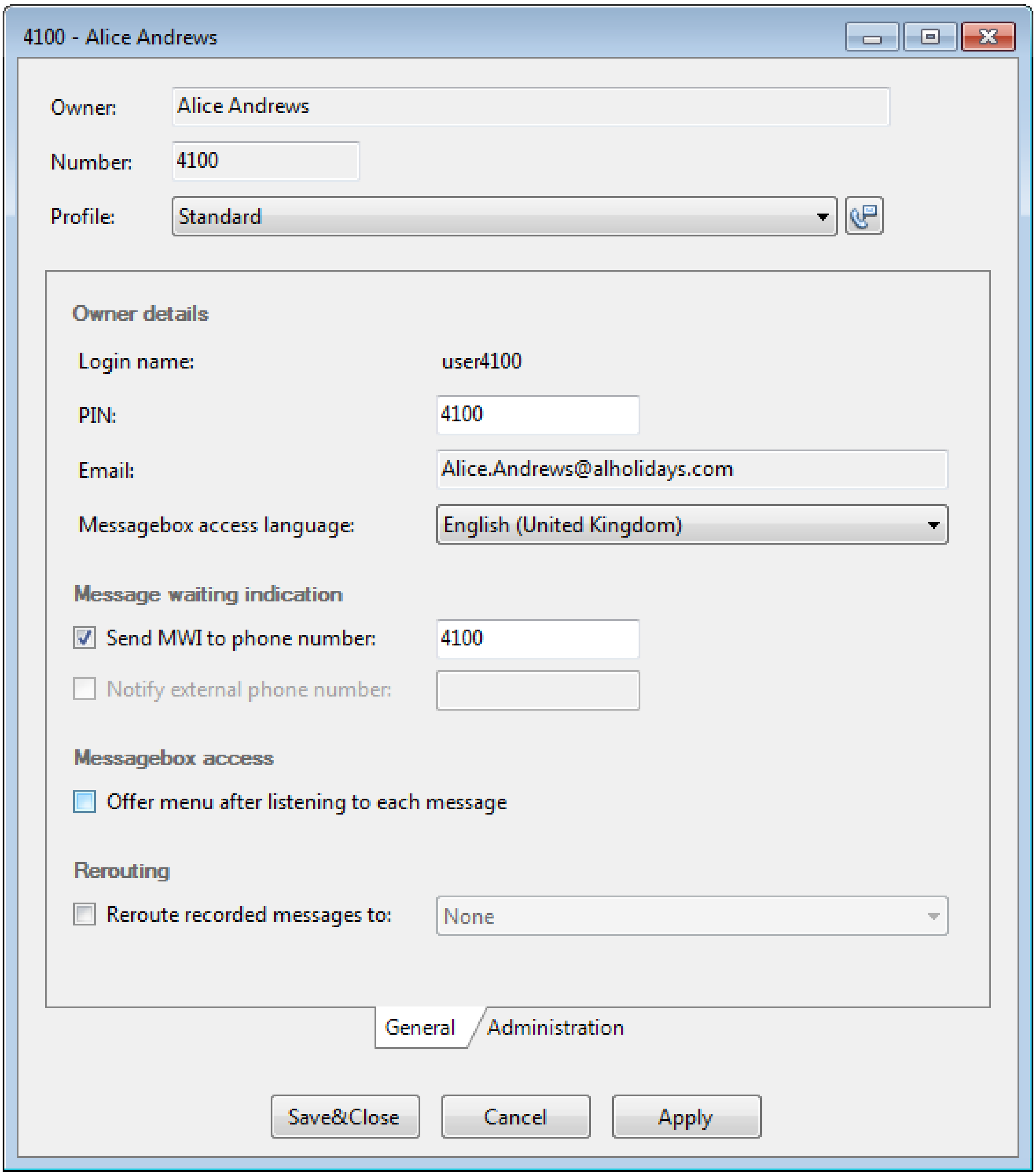
8.1.9.1. Voicemail access

Access right to the voicemail module is granted by the BCT System Settings.

1. Login to BCT System Settings as Administrator.

2. Select the Company Directory tab search for the user and click edit to enter the properties. The Personal Identification Number (PIN) field is used by the voicemail application. Authorization to the message box (from another extension) is controlled by this PIN. Enter a PIN and click Apply to save the changes.

3. When a messagebox is created, by default the message menu for handling the messagebox via the phone is enabled. The message menu plays the prompts to guide the user through the menu. This can be switched off. Start the BCT Supervisor Dashboard and select the messagebox. See Figure 8-34 Messagebox Properties.



4100 - Alice Andrews

Owner: Alice Andrews

Number: 4100

Profile: Standard

Owner details

Login name: user4100

PIN: 4100

Email: Alice.Andrews@alholidays.com

Messagebox access language: English (United Kingdom)

Message waiting indication

☑ Send MWI to phone number: 4100

☐ Notify external phone number:

Messagebox access

☐ Offer menu after listening to each message

Rerouting

☐ Reroute recorded messages to: None

Figure 8-34 Messagebox Properties

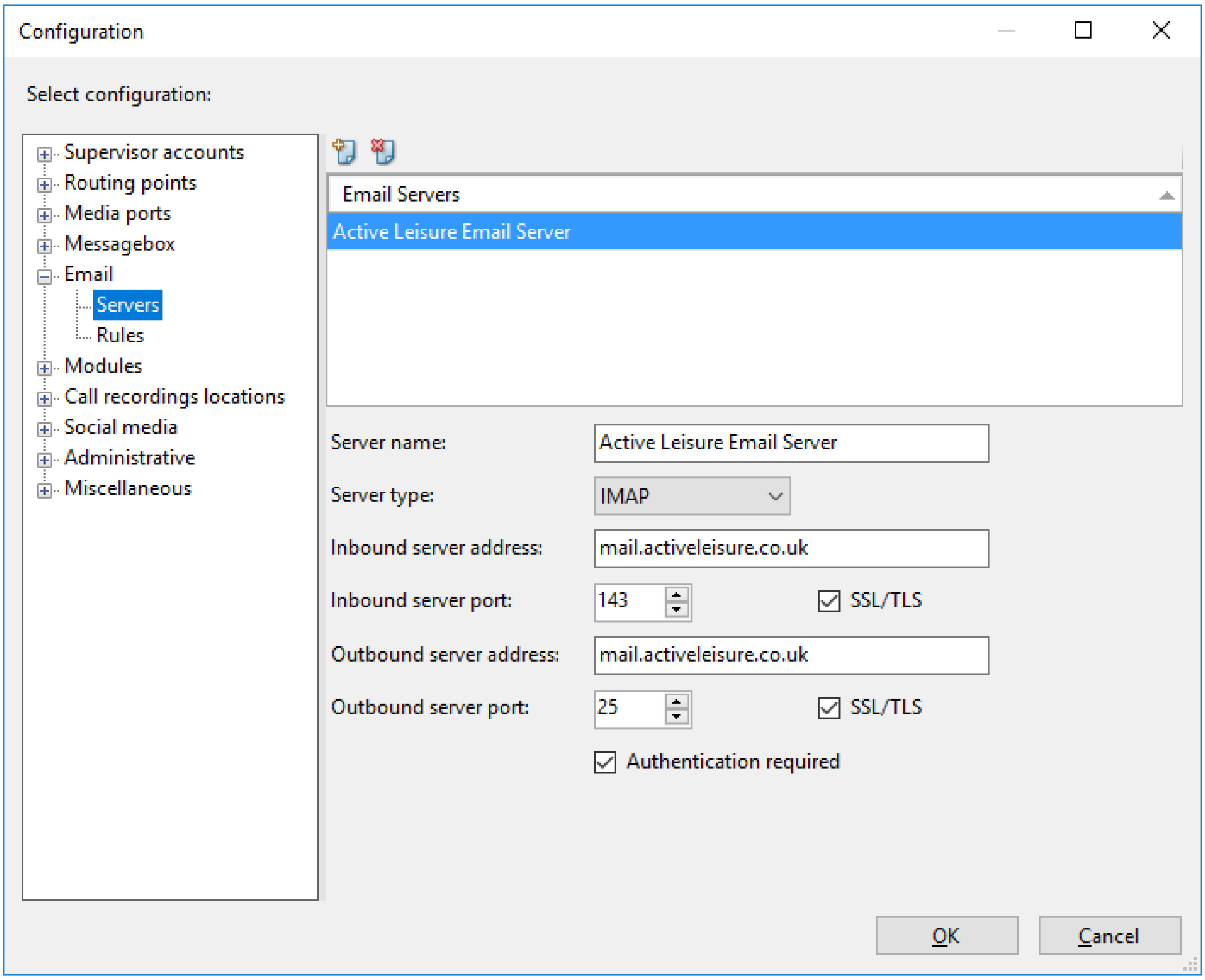
8.1.10. Email integration

BCT can be configured to integrate with an email server to:

- Allow users to send their voicemail to their email (Unified Messaging).
  See 8.1.10.1 Configure Voicemail to Email (Unified Messaging).

- Automatically generate reports to be sent via email.
  See 8.2.3 Email Integration for the Reporting module.

If you want to use one of these licensed options, you must configure the outbound email server. Login to the BCT Supervisor Dashboard as Administrator. Select **Email Servers** via Tools Configuration and select **New** from the tool bar. The following window appears:



Server name: Active Leisure Email Server

Server type: IMAP

Inbound server address: mail.activeleisure.co.uk

Inbound server port: 143 ☑ SSL/TLS

Outbound server address: mail.activeleisure.co.uk

Outbound server port: 25 ☑ SSL/TLS

☑ Authentication required

Figure 8-35 Email Server window

For BCT email Server configuration, both outbound and inbound server address needs to be filled in. Outbound is used for message transfer to the email server, for distributing Supervisor Dashboard reports via email and for sending alarm notifications via email. Inbound is used for email routing by BCT (See BCT Administrator Guide).

Note: If McAfee is used, you may encounter an error because McAfee blocks all outgoing messages sent by any program that it does not recognize. For more information, please refer to section 11.3.5.1 McAfee blocks email port.

8.1.10.1. Configure Voicemail to Email (Unified Messaging)

When an email server is configured in the BCT Supervisor Dashboard, BCT users can send their voicemail to their email account. To be able to do so, the following conditions must be met:

1. The address of the email server in BCT Supervisor Dashboard must be defined.

2. A system email account must be defined in BCT Supervisor Dashboard. See BCT Administrator Guide.

3. The option "Email to owner" in the MessageBox Profile should be checked.

4. The email address of the user must be added in the BCT company directory via BCT System Settings.

5. The Email Integration license must be loaded (See 8.1.3 Activate BCT licenses).

6. To customize the email or to make use of other language than the default English, please check Appendix S – Customizing email notification.

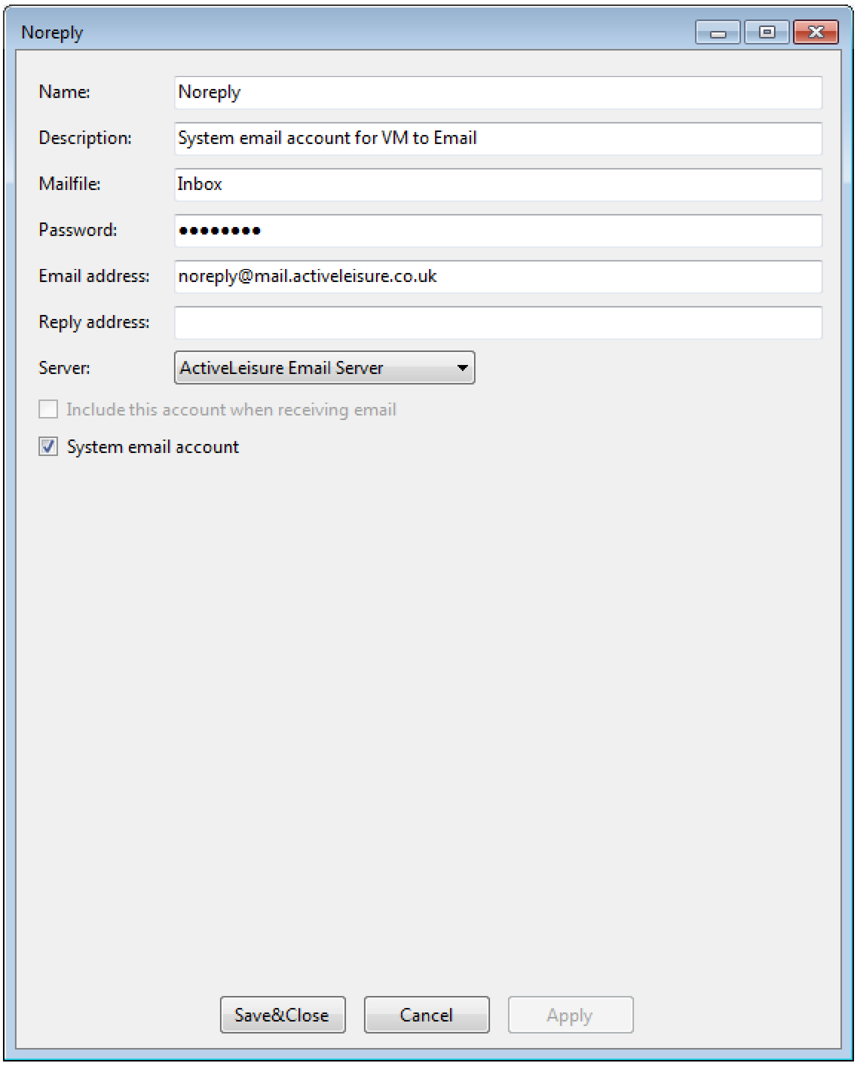
Voicemail forwarded to email is sent on behalf of the system email account that has to be configured in the BCT Supervisor Dashboard. This email account has to be an existing email account on the mailserver. Receivers of an automatically generated message like the voicemail, cannot reply. Information which email account to use must be obtained from the IT department.

Creating a system email account for BCT

1. Start the BCT Supervisor Dashboard, and log in.

2. Select the Email accounts in the Call Flow module.

3. Create a new email account and mark the **System email account** check box.



Noreply

Name: Noreply

Description: System email account for VM to Email

Mailfile: Inbox

Password: ••••••••

Email address: noreply@mail.activeleisure.co.uk

Reply address:

Server: ActiveLeisure Email Server

□ Include this account when receiving email

☑ System email account

Figure 8-36 Email account properties in BCT

- *Name*: Email account name

- *Description*: can be any meaningful description

- *Mailfile*: the folder on the IMAP server to read email messages from. For the system email account, it is not required.

- *Password*: the password as specified in the Email client account information.

- *Email address*: an existing mail address on the mailserver that is configured as no reply account

- *Reply address*: used for ‘regular’ email accounts.

- *Server*: select the email server the system account is created for. See 8.1.10 Email integration.

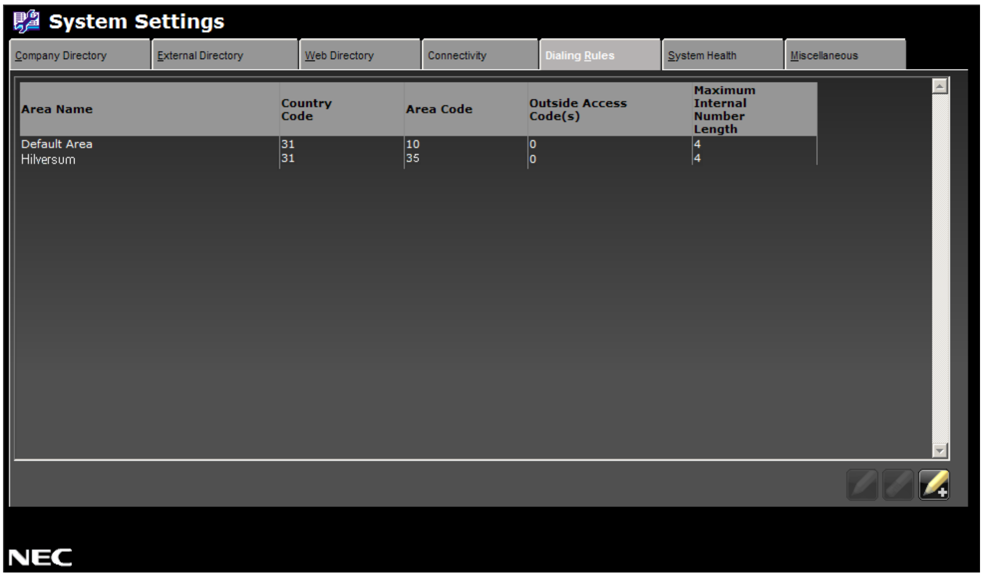
- Include this account when receiving mail: used for ‘regular’ email accounts.

A System email account gets the following icon: ✉ .

8.1.11. Dialing Rules

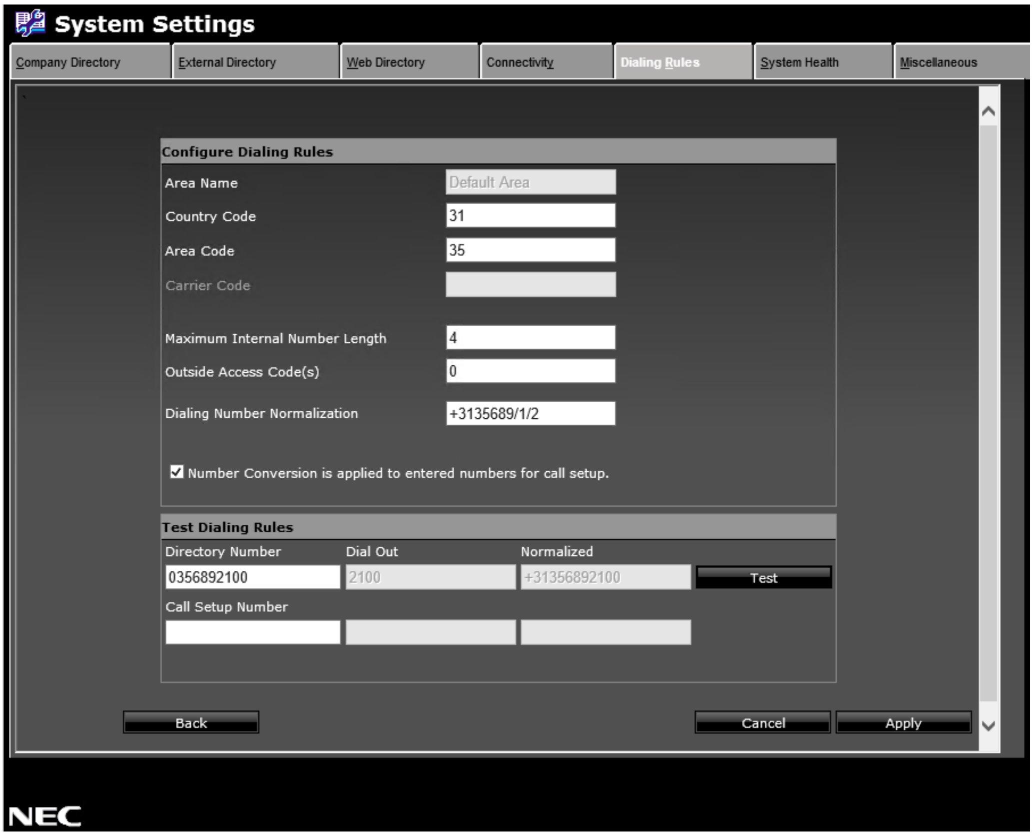
Initially, the dialing rules for the default area have been created via the Configuration Wizard. See 8.1.1 Using the Configuration Wizard.

1. If you click the **System Setting** / **Dialing Rules** tab, the currently defined areas are shown (initially only the default area).



Area Name	Country Code	Area Code	Outside Access Code(s)	Maximum Internal Number Length
Default Area	31	10	0	4
Hilversum	31	35	0	4

Double-click on an area to modify it, or press the **New** button to add an area. The Configure Dialing Rules window appears.



Configure Dialing Rules

Area Name	Default Area
Country Code	31
Area Code	35
Carrier Code	
Maximum Internal Number Length	4
Outside Access Code(s)	0
Dialing Number Normalization	+3135689/1/2

☑ Number Conversion is applied to entered numbers for call setup.

Test Dialing Rules

Directory Number	Dial Out	Normalized
0356892100	2100	+31356892100

Call Setup Number

Figure 8-37 System Settings - Configure Dialing Rules

See 18 Appendix H – DIALING RULES AND NUMBER CONVERSION for more information.

2. Fill in the fields:
   - Area Name
   - Country Code (normally you would not modify this)
   - Area Code

Note: *Fill in the Area Code as presented in the international number format, usually without the National Access Code. For countries where local numbers include the Area Code, this field must be left empty.*

- Carrier Code
  Identifies the operator (carrier) that the system is using (Currently only applicable for Brazil).
- Maximum internal number length
- Outside access code (PBX trunk access code)
- Dialing Number Normalization
  Use this field to prevent that calls are made via a trunk when an local extension is called as external number. Ranges of external numbers can be defined which must be converted to extension numbers for outgoing calls. See Note 2.
- In case you are modifying the Default Area:
  Option "Number conversion is applied to entered numbers for call setup".
  See 8.1.1 Using the Configuration Wizard step 16.

1. You can **Test** the Dialing rules before pressing the Apply button.
   Enter the numbers you want to test in the Directory Number field or Call Setup Number field and
   press the Test button. The results are shown in the fields Dial Out and Normalized.

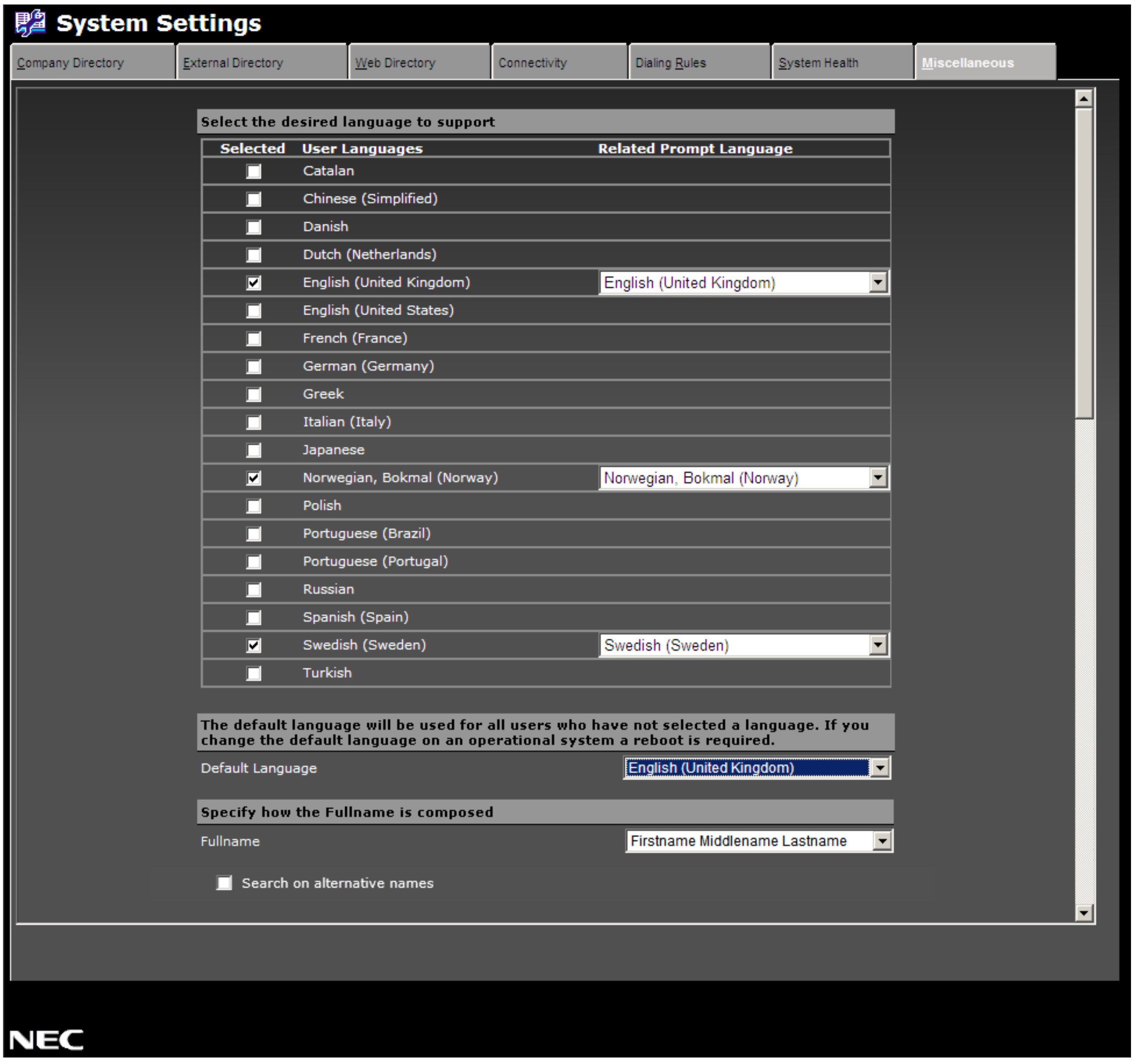
2. Click **Apply** to save and activate the new dialing rules.

Note: Trunk access codes: For a number of PBX types, numbers over the trunk lines must be prefixed with an access code to get correct phone number information. See in 18.3.2 Trunk Line access codes whether this is the case for your PBX.

Note 2: Dialing Number Normalization.
Enter a comma-separated list of external number blocks which are related to internal extensions, in the format <prefix>[/block]*, [<prefix>[/block]*]*.
Prefix is the part that is removed from the number in E164 format to obtain the extension number.
Block indicates the first digit(s) of a block of extensions.
Example: you enter +3135601,+3135602/2/5
- +3135601 means: all numbers +3135601xxxx are dialed out as xxxx,
- +3135602/2/5 means:
  - all numbers +31356022xxx are dialed out as 2xxx and
  - all numbers +31356025xxx are dialed out as 5xxx.

Restriction: use this feature only when blocks of extensions are assigned. When relation between external number and extension is per individual extension, or there are many very small blocks, it is better to configure proper routing in the PBX.

8.1.12. Miscellaneous



Select the desired language to support

Selected	User Languages	Related Prompt Language
□	Catalan	
□	Chinese (Simplified)	
□	Danish	
□	Dutch (Netherlands)	
☑	English (United Kingdom)	English (United Kingdom)
□	English (United States)	
□	French (France)	
□	German (Germany)	
□	Greek	
□	Italian (Italy)	
□	Japanese	
☑	Norwegian, Bokmal (Norway)	Norwegian, Bokmal (Norway)
□	Polish	
□	Portuguese (Brazil)	
□	Portuguese (Portugal)	
□	Russian	
□	Spanish (Spain)	
☑	Swedish (Sweden)	Swedish (Sweden)
□	Turkish	

The default language will be used for all users who have not selected a language. If you change the default language on an operational system a reboot is required.

Default Language: English (United Kingdom)

Specify how the Fullname is composed

Fullname: Firstname Middlename Lastname

□ Search on alternative names

Figure 8-38 Miscellaneous window part 1

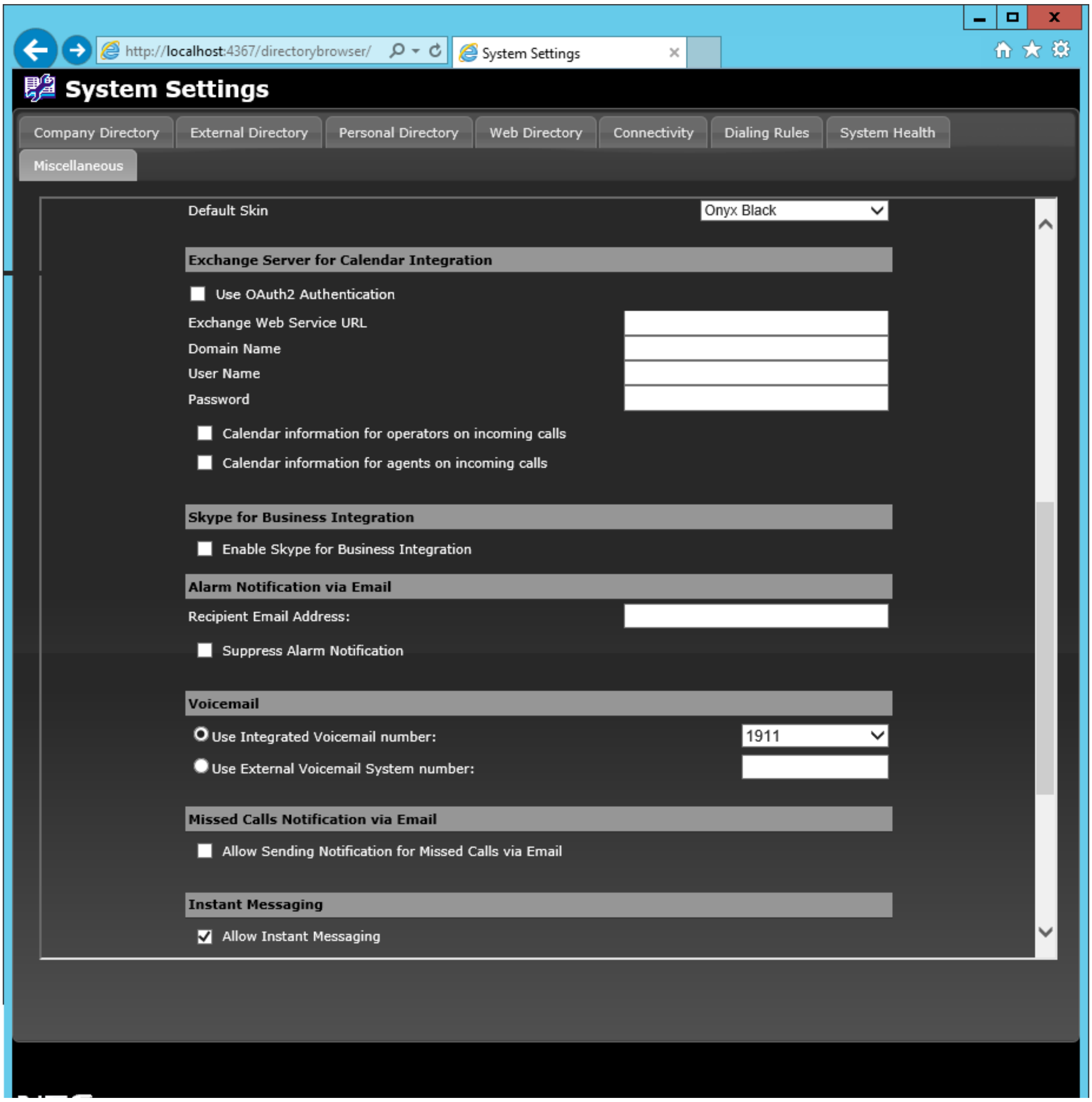
The miscellaneous part of the administrator window can be used to change the system default settings.

1. Language: The displayed **licensed** languages can be used, and a default language can be defined.

2. Fullname Composition: This defines the composition of a contact name as shown in the directory. The composition differs per language / country.

3. Search on alternative names: If this is selected, two alternative names can be specified for each user. (This can for instance be used for Japanese Hiragana / Katagana variants).

   Note that:
   - The fullname composition will apply to each of these alternatives as well.
   - The search function of the directory will also include these alternatives.



System Settings

Default Skin: Onyx Black

Exchange Server for Calendar Integration

□ Use OAuth2 Authentication

Exchange Web Service URL

Domain Name

User Name

Password

□ Calendar information for operators on incoming calls

□ Calendar information for agents on incoming calls

Skype for Business Integration

□ Enable Skype for Business Integration

Alarm Notification via Email

Recipient Email Address:

□ Suppress Alarm Notification

Voicemail

○ Use Integrated Voicemail number: 1911

○ Use External Voicemail System number:

Missed Calls Notification via Email

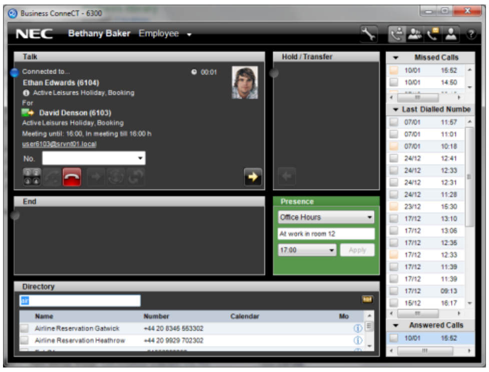
□ Allow Sending Notification for Missed Calls via Email

Instant Messaging

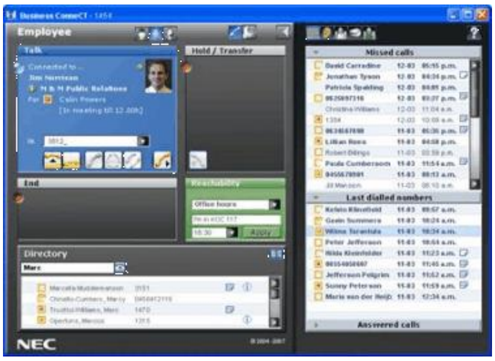
☑ Allow Instant Messaging

Figure 8-39 Miscellaneous window part 2

4. Skins: You can change the look and feel of the BCT client and the Directory Browser. You select a skin for **all** clients (default is “Onyx Black”). The new skin will be effective for all users who logged in after this change.



Onyx black skin



Black Velvet skin

5. Exchange Server: For Calendar Integration and user calendar popup for operator (see also 21 Appendix K – EXCHANGE INTEGRATION)
When checkbox “Use OAuth2 Authentication” is not checked the following fields must be entered:

    - Exchange Web Service URL
      The URL to access the Exchange Web service. Typically https://<exchangeservername>/EWS/Exchange.asmx

    - User Name
      It is advised to make a separate Windows account for this user. Per default the user has sufficient rights to access the Exchange Webservice for free/busy information. However, for user calendar popup functionality impersonation privilege and reviewer access rights must be assigned to the user.

    - Password
      The password of this user. It is necessary to set the Windows Active Directory User option "Password never expires" to On.

    - Domain Name
      The name of the Domain.

   When checkbox “Use OAuth2 Authentication” is checked then the following fields must be entered:

    - Email Address
      The Email Address of an (administrator) user having permissions for Office 365 Exchange Online on reading calendars.

    - Tenant ID
      The Tenant ID (Directory ID) of the Azure account.

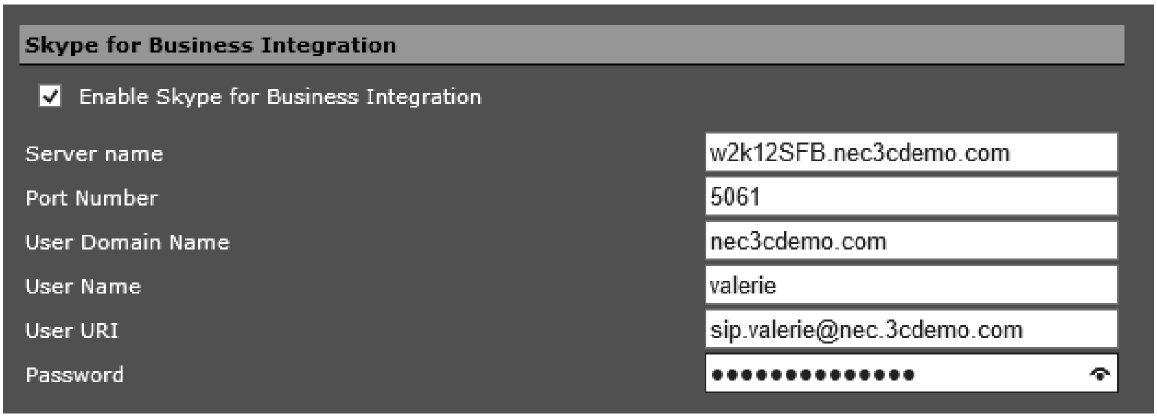
    - Client ID
      The Client ID (Application ID) associated to the application name.

- Client Secret
  The Client Secret generated to access and associated to the application.

To enable user calendar popup functionality for operators also check the checkbox “Calendar information for operators on incoming calls”.
To enable user calendar popup functionality for agents also check the checkbox “Calendar information for agents on incoming calls”.
Additional Exchange privileges are required, see 21 Appendix K – EXCHANGE INTEGRATION for more information.

When Skype for Business integration is enabled, the exchange integration component is used to retrieve calendar information for all Business ConneCT users that do not have an employee role.

6. Skype for Business Integration: For BCT Presence and IM Skype for Business Integration check the ‘Enable Skype for Business Integration’ checkbox and enter the following fields:



Skype for Business Integration

☑ Enable Skype for Business Integration

Server name	w2k12SFB.nec3cdemo.com
Port Number	5061
User Domain Name	nec3cdemo.com
User Name	valerie
User URI	sip.valerie@nec.3cdemo.com
Password	●●●●●●●●●●●●●●

- Server Name
  The hostname or IP address of the Skype for Business Server.

- Port Number
  The port number on the Skype for Business Server for communication with the BCT Server. Default Skype for Business is using ‘5061’.

- User Domain Name
  The Windows domain name associated to the ‘BCT User’.

- User Name
  The Windows user name of the ‘BCT User’.

- User URI
  The SIP URI of the ‘BCT User’. The syntax is typically: ‘sip:user@domain’

- Password
  The windows password of the ‘BCT User’.

  The ‘BCT User’ is a user configured by the Skype for Business administrator and is used by the BCT server for communication with the Skype for Business Server to retrieve the presence states of other Skype for Business users.

  When ‘Enable Skype for Business Integration’ is checked it is possible to set the Skype for

Business SIP URI for every user in the BCT Company Directory.
The BCT Server will retrieve the Skype for Business presence for every user with a SIP URI configured in BCT.
Default the Skype for Business SIP URI is set to 'sip:' followed by the email address of the contact.

Note: *Skype for Business Integration requires the BCT External Presence Integration license. If the BCT External Presence Integration license is not available the Skype for Business Integration checkbox will be disabled.*

7. Alarm Notification via Email: When the recipient email address is filled in, the recipient will get emails about state transitions of the system: starting/started, raised alarms and resolved alarms. You can enter multiple email addresses separated by "," or ";".

   The frequency of the notifications can be tuned by using the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common Files\NEC\Services\AlarmingService.WinService.exe.config" to change the values of the keys:

   - InitialDelay <m>: the first alarm notification is not sent earlier than <m> minutes after a restart. Default is 6 minutes.

   - AlarmNotifyDelay <n>: after the first alarm occurs, the system waits for <n> more seconds to collect subsequent alarms in the same notification message. Default is 30 seconds.

   - AlarmNotifyInterval <p>: after an alarm notification message has been sent, the system waits for <p> minutes before a next alarm notification message is sent. Default is 30 minutes.
     State changes (from healthy to unhealthy or v.v.) are notified immediately.

   - AlarmExpiryPeriod <q>: alarms raised more than <q> hours ago are ignored. Also alarms raised before a system restart are ignored.

   - DirectAlarmIDs: alarms with these ID's will bypass the above delays and will be send direct to the recipient email address. Multiple ID's can fill filled in separated by commas. The Alarm ID's can be found in 11.4.3 List of BCT Alarms.

   Alarm emails are always saved as HTML file, independent whether sending of email did succeed (name example 'AlarmEmail_20170818114952.html').
   Both the location as well as purge (cleanup of old files) behavior can be configured by using the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common Files\NEC\Services\AlarmingService.WinService.exe.config" to change the values of the keys:

   - AlarmEmailFolder: the name of the subfolder under "C:\NEC\Data Files" where the HTML files are saved. Default is "Alarming Emails".
     Note that when value contains full folder path this folder is used as save location.

   - AlarmEmailRetentionPeriod: retention period in days defines how long files should be retained. Default is "" (empty means keep them all).
     The purge (cleanup) of expired email files will occur only when triggered by new saved alarm email file.

When 'Suppress Alarm Notification' is selected, no notification messages are sent. It is good practice to select this setting while maintenance is being done on the system.
Alarm Notification uses the Email Server and System Email Account (sender address) as configured for BCT, see 8.1.10 Email integration.

8. Voicemail:
   BCT is equipped with an internal voicemail system. If you require an external voicemail system, select that option. In both cases, enter the voicemail access number in the appropriate field. BCT makes this number available to all users as the default voicemail number.
   If more than one internal voicemail number is defined, select the number to use as the default for users.

Note: *It's also possible to give a user voicemail only. You can create a voicemail box for the user. The user can then access the voicemail part of BCT with their phone, but can't log in to BCT.*

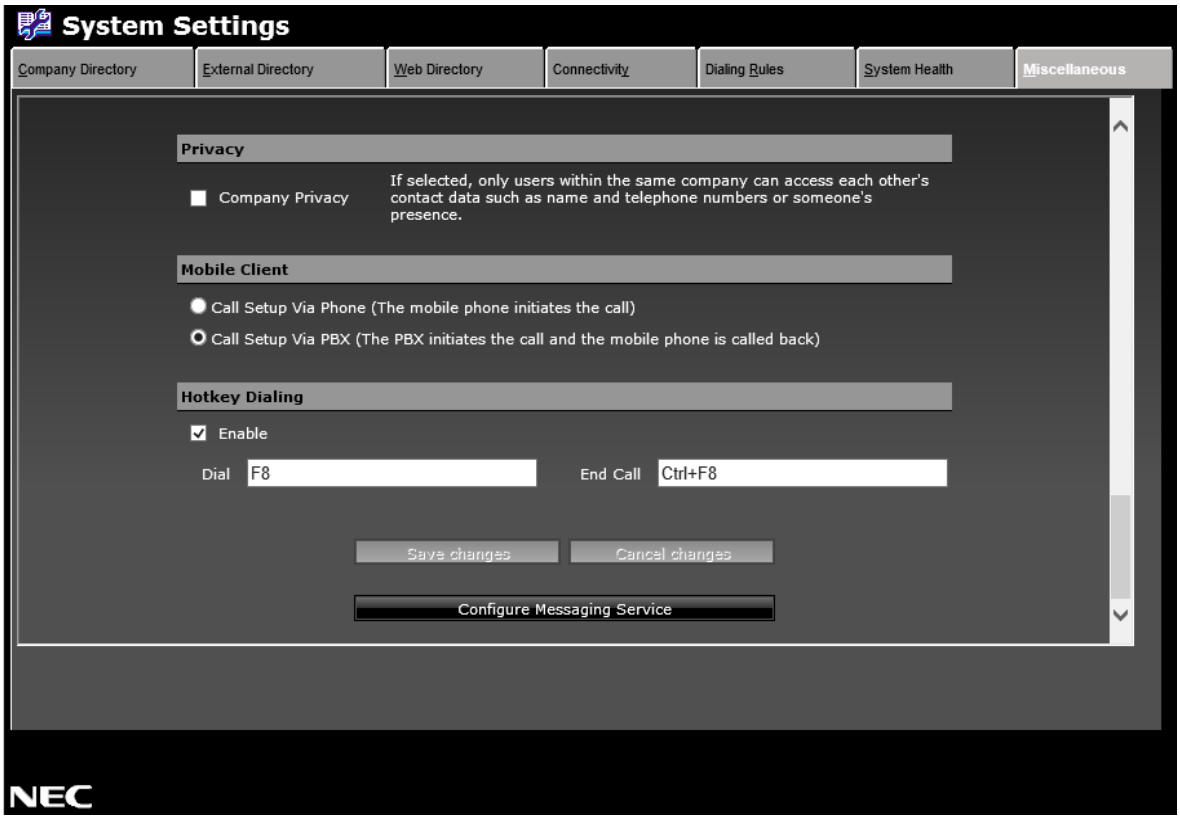
Note: *Internal and external voicemail cannot be used in parallel. In case you select external Voicemail, you cannot use the MessageBox Module in a callflow (See BCT Administrator Guide).*

9. Missed Calls Notification via Email:
   If "Allow Sending Notification for Missed Calls via Email" is checked the BCT users will have the possibility to configure whether the system will notify them by email when they miss a call. The configuration will be available for each user individually in Desktop Client. For more information see BCT Supervisor Guide. To customize the email or to make use of other language than the default English, please check Appendix R – Customizing email notification.

10. Instant messaging: If this checkbox is cleared, BCT users will not have access to Instant Messaging.
    Note: By default, a notification sound is played if a user receives a new instant message. To disable these sounds, add the following to RemotingService.WinService.exe.config:

```
<add key="Sound_IMNotification" value="" />
<add key="Sound_NewInstantMessage" value="" />
```

After setting this, a reboot of the BCT server is required.



Privacy

□ Company Privacy — If selected, only users within the same company can access each other's contact data such as name and telephone numbers or someone's presence.

Mobile Client

○ Call Setup Via Phone (The mobile phone initiates the call)

● Call Setup Via PBX (The PBX initiates the call and the mobile phone is called back)

Hotkey Dialing

☑ Enable

Dial: F8 End Call: Ctrl+F8

Figure 8-40 Miscellaneous window part 3

11. Company Privacy. If this checkbox is activated, then users can only see contact data (such as name, number, presence) of other users, if these other users belong to the same company.

12. Mobile Client Call Setup: This system setting controls the call setup mode of the BCT Mobile client.

    - Call setup via PBX (PBX initiates the call and the Mobile phone is called back)

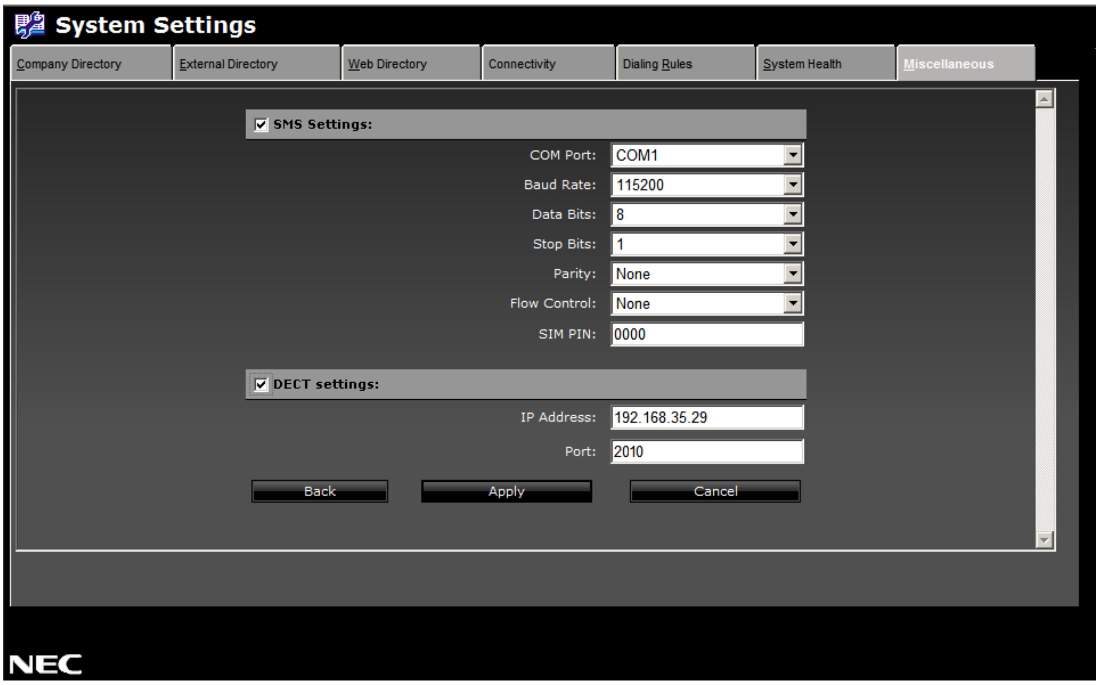
    - Call setup via Phone (The Mobile phone initiates the call).

***Note:** This only works for dialable numbers (external numbers without a Trunk Access Code)*

13. Hotkey Dialer Configuration
    By default this feature is enabled and it will offer (enable) the hotkey dial support that is integrated in the Desktop Client.
    To change the ‘Dial’ and ‘End Call’ hotkey defaults press the requested hotkey (when focus in in the related text box) and ‘Save changes’.

    ***Note:** The default settings can be changed (overruled) locally in the Desktop Client.*

14. If you click the **Configure Messaging Service** button, you can specify whether BCT users will have the option(s) to send a message to a business phone (DECT) or mobile phone (SMS). You may need to scroll down in the Miscellaneous main window to see this button.



☑ SMS Settings:

COM Port: COM1

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: None

Flow Control: None

SIM PIN: 0000

☑ DECT settings:

IP Address: 192.168.35.29

Port: 2010

Figure 8-41 Miscellaneous window - Configure Messaging Service

Mark the required check box(es).

For SMS messaging you need a GSM modem (e.g. the Wavecom Fastrack M1306B).
Enter the SIM PIN of this GSM box.

For DECT messaging enter the IP address of the IP DECT device (DAP Controller (DMLS)).

After you made changes, first click **Apply Changes** then **Back** to return to the Miscellaneous main window.

15. Select **Save changes** to save the settings.

8.1.13. BCT Mobile Client application

The BCT Mobile Client application is an integrated part of the BCT server platform. It is automatically installed. After the BCT server installation is finished, some configuration is needed.

BCT Server Configuration

The BCT Mobile Client application is meant to be used from the internet. As a consequence:

- The BCT server must be connected to the internet
  There are several possibilities to connect the BCT server to the internet.
  Details are described in BCT Mobile Client Network Security

- It is strongly advised to configure the BCT Mobile Client application to run under SSL/TLS in order to support secure HTTPS internet connections. Depending on the configuration chosen to connect the BCT server to the internet, a certificate must be installed at the BCT Server or at a proxy server. Details are described in BCT Mobile Client Network Security.

Note: *Important for BCT Mobile Client: use a certificate that is supported by the mobile devices. On most mobile phones certificates can be downloaded, but nowadays mobiles have a number* *of common certificates on board. The easiest way: check the certificates on your mobile devices and buy a certificate known by the mobiles.*

- To protect against unauthorized access of BCT web pages, see chapter 22 Appendix L – HOW TO LIMIT PUBLIC ACCESS TO BCT WEB PAGES AND WEB APPLICATIONS.

User Configuration on the server (via System Settings)

To be able to access the BCT Mobile Client application:

- A user must login with a username and password.
  The BCT Mobile Client uses BCT Basic Authentication (default). See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.
  Empty passwords are allowed (but we strongly advise against it, for security reasons).

- A user must be granted the BCT role '[Employee]'.

- Option 'Disable Presence Settings' must be switched off to use the Presence Settings options.

Mobile client Configuration
See 9.5 Mobile Client.

8.1.14. Disable AM/PM time for callback options.

When the client has the option to schedule the time he will be called back, the system will prompt him first to choose AM or PM. This happens only when the call flow language is English (US), English (UK) or Greek. In order to disable this behavior and accept only 24 hour input, execute the following steps:

1. Open the Configuration Manager and select the configuration file: "C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config".

2. Enable/Include:

   ```
   <add key="Force24HoursInput" value="True"/>
   ```

3. Save the file.

4. Restart UCSRuntime service.

8.1.15. Failure recovery

In case failures occur during a start of the UCS Runtime service, or in case UCS Runtime service becomes unresponsive, the service manager of windows will try to restart this service twice. When both restarts fail, BCT (Monitoring service) will continue to try to restart the UCS Runtime service for another three times. When all three restart attempts fail again, an alarm will be raised that will be handled like all other BCT alarms.

This default behavior can be changed by executing the next steps:

1. Open the Configuration Manager and select the configuration file: "C:\Program Files (x86)\Common Files\NEC\Services\ MonitoringService.WinService.exe.config".

2. Enable/Include:
   <add key=" Recovery.MachineRebootEnabled" value="true"/>

3. Save the file.

4. Restart Monitoring Service.

Now the Monitoring Service will not retry 3 times to start the UCS Runtime service, but instead will force a restart of the BCT server. This will be signaled by a windows message (appearing for 10 seconds) that the machine is about to restart and next the server is actually rebooted.
Especially in standard HA (High Availability) environmnets this can avoid longer downtime of UCS Runtime service.

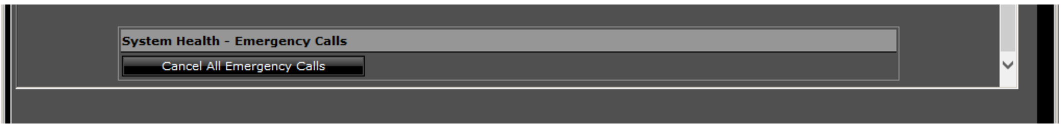
8.1.16. Emergency Number calling

NOTE*: This functionality is not a replacement or substitute for other emergency procedures and configurations but merely an addition to existing emergency procedures. Be aware that calling or break-in into a caller requesting emergency assistance can interfere or compromise with emergency prodecures.*

When a user calls the emergency number from an extension monitored by Business ConneCT either:

1. A notification pop-up will be given to all operator desktop clients logged-in at that moment.
   This Notification popup contains the emergency number being dialed, the extension number that dialed the emergency number, the user name of the associated user, location (building) of the associated user and present state (if defined in System Settings).
   The operator can then take action to contact the caller for more information.
   When no operator was logged-in at the time the emergency number was called an alarm will be raised and when configured an email will be send directly to the recipient for alarm notifications, see 8.1.12 Miscellaneous.
   This alarm will be lowered when an operator logs in.
2. A specified notification number will be called to announce that one or more users (maximum three) have called the emergency number.
   This notification number can be an internal or external number.
   The notification number will only be called when specified and no operators are logged in.
   Next to calling the notification number an alarm will be raised and when configured an email will be send directly to the recipient for alarm notifications, see 8.1.12 Miscellaneous.
   This alarm will be lowered when the notification number is called, answered and the announcement is at least played once completely.
   The announcement will be repeated until the call is disconnected.
   If the call to the notification number is not answered within 2 minutes, fails or the announcement is not listened to at least once, the call is repeated after 1 minute.

When one or more emergency notifications are present, they can all be cancelled from the system health page. Popups on operator/call to notification number will be cancelled.



System health page – Cancel Emergency notifications

Note that monitoring (all or less) extensions can be selected: see section 8.1.8 Selective Monitoring.

8.1.16.1. Define the emergency Number

To define the emergency number:

1. Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example.
   Most likely location: C:\Program Files (x86)\NEC\UCS-Module\Server.
   And locate the commented key, move it out of the comment block and assign the required value:

   ```
   <add key="EmergencyNumber" value="112"/>
   ```

2. Change value to “<required-emergency-number>” (the value for the emergency number, in E.164 format for external numbers or digits for an internal number) and save the file.

3. The value will be active within at maximum 10 seconds.

Note: If the key was already outside a comment block it is also possible to use the Configuration Manager to change the value (select the configuration file: “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config”).

8.1.16.2. Define the Emergency Notification Number

To define the emergency notification number:

1. Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example.
   Most likely location: C:\Program Files (x86)\NEC\UCS-Module\Server.
   And locate the commented key, move it out of the comment block and assign the required value:

   ```
   <add key="EmergencyNotificationNumber" value="2222"/>
   ```

2. Change value to “<required-emergency-notification-number>” (the value for the notification number, in E.164 format for external numbers or digits for an internal number) and save the file.

3. The value will be active within at maximum 10 seconds.

Note: If the key was already outside a comment block it is also possible to use the Configuration Manager to change the value (select the configuration file: “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config”).

8.2. Contact Center configuration

The initial configuration of the Contact Center part of NCT is described in section 8.1.6 Start and configure the BCT Platform. More detailed information on how to configure the Contact Center can be found in the BCT Administrator Guide.

8.2.1. Wallboards (optional)

This requires a Wallboard license.

Wallboards display real time group information and are intended to be positioned where agents can see them. There are two ways of establishing a connection to the wallboard: via V.24 or via Ethernet (depending on the type of wallboard). There are three types available: 2 hardware wallboards and one software wallboard. The supported hardware wallboards are DataDisplay wallboards and MessageMaker wallboards. The MessageMaker wallboard can also be connected via an IP connection. The software wallboard is a Microsoft PowerPoint based solution.

For information on how to install the wallboard's hardware and software, please refer to the documentation that comes with the product.

Hardware wallboards

If a hardware wallboard is connected to the BCT Server, the following services must be started:

- NEC UCS Wallboard Service: This service is responsible for the wallboard module. The Start-up Type after installation is "Automatic".

- NEC Wallboard API Service: This service is triggered via the wallboard control. When a "Start" wallboard is performed in the BCT Supervisor Dashboard, the service should change to "Started". The Start-up Type after installation is "Manual". You may want to change this to "Automatic".

If a hardware wallboard is connected to a client computer (that hosts the wallboard software), then the NEC UCS Wallboard service must be started on the SERVER and the NEC Wallboard API Service must be started on the CLIENT.

To open the Services icon, select Start > (Settings >) Control Panel. Double click Administrative Tools, double click Services.

Application	UDP Port	Target Machine
Wallboard Manager Service	51170	Server
For every defined Wallboard	51171 and up	Clients
Wallboard API	51070 and up	Server/Clients

Table 8-1 UDP port numbers used by wallboards components

Software wallboards

If a software wallboard is connected to the BCT Server, the following service must be started:

- NEC FrontEnd Service: This service is responsible for delivering wallboard information to the Soft Wallboard Client. The Start-up type after installation is "Automatic".

Application	TCP Port	Target Machine
FrontEnd Service	32011(SSL), 32010	Server

Table 8-2 TCP port numbers used by software wallboards

If the Soft Wallboard needs to use a different TCP port than the default configured port, please change this in the following configuration file on the BCT server: FrontEnd.WinService.exe.config. Be sure that when changing this port you also must indicated this changed TCP port in the Soft Wallboard Client (please refer to BCT Administrator Guide for more information).

Controlling a wallboard

Controlling a wallboard is integrated in the BCT Supervisor Dashboard application. In the BCT Supervisor Dashboard – Explorer view, left mouse click **Wallboards** under **Resources**. Now you see an overview of the wallboards that are already configured (if any). If you want to create a new wallboard, right mouse click in the pane at the right side of the Explorer pane and click **New**.

Please refer to the BCT Administrator Guide, chapter "Wallboards" for information on how to configure a wallboard and to the BCT Supervisor Guide for more information on how to configure wallboard messages.

8.2.2. Configure Email Routing

BCT can distribute Email among the Contact Center agents.

One or more Email addresses are announced to the customers of the Contact Center. All Emails that are sent to the Email address of the Contact Center will be distributed among the agents that are assigned to the selected router.

Note: *The following procedure is described in more detail in the BCT Administrator Guide.*

1. An Email server must be installed in the same network as the BCT server and client computers.
   The Mail server must be configured in such a way that unread and read mail can be sent to agents.
   The Mail server must support SMTP (for outgoing email), either POP3 or IMAP (for incoming email) and/or Microsoft Graph (for Microsoft Office365 – Outlook).

   The following mail servers have been tested and are working correctly:
   - Microsoft Exchange Server
   - Exchange Server of Microsoft Office365
   - Google Gmail
   - hMailServer

2. Create one or more Email accounts on the Email server. These Email accounts are the Email addresses that must be announced to the customers of the Contact Center.

   Note: *Do not create these accounts on the Email clients, only on the server.*

3. Create an Email account for each agent that is used to distribute Email to on the Email client software.
   Note that read as well as unread mail should be offered to the client.
   The Email address of the agent must be entered in the agent properties in the BCT Supervisor Dashboard.

4. Create an Email server in the BCT Supervisor Dashboard.

5. Create an Email account in the BCT Supervisor Dashboard.

6. Create at least one Email rule for the Email account.

Note1: *If you want the name of the attachment in the email to be "<email address>.txt" instead of <sender info>.text", do the following:*

- Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example. Most likely location: C:\Program Files (x86)\NEC\UCS-Module\Server.
- enable / include:

```
<add key="EmailAddressAsAttachmentFilename" value="true"/>
```

Note2: *If you want the email, received by an agent, to show as being sent by a customer in stead of being sent by the configured account, execute the following steps:*

1. Open the Configuration Manager and select the configuration file: “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config”.

2. Locate the key: ShowCustomerEmailAddress

3. Change value to "From" or "OnBehalf" or ""
   When added using "From", an agent will see the customer address in the ‘From’ field of its email client. When added using “OnBehalf”, an Outlook-Client will show the mail as being sent by the customer ON BEHALF OF the email-account-address.
   Note: it depends of the email-client if this functionality works, some email clients (e.g Windows 10 mail) will not send the reply to the router as is required but to the party in the ‘From’ field.

4. Press button Save to store the value.

5. Restart UCS Runtime service.

8.2.3. Email Integration for the Reporting module

BCT can automatically send reports via email. These emails have to be sent by an email application and account on the BCT server. To enable this, an Email Server and a system email account needs to be configured. The same account as used for Voicemail to Email can be used. See 8.1.10.1 Configure Voicemail to Email (Unified Messaging).

8.2.4. Social Media Integration

BCT offers functionality for Social Media Integration. This means the ability to route Social Media messages (like WhatsApp messages, Twitter Direct messages, Facebook Messenger, iMessage and SMS) to the Contact Center agents.

For more information on how to configure Social Media see BCT Administrator Guide.

At this moment BCT has certified “SaySimple” (a Dutch company) as Social Media provider.
You should request an account in order to use this functionality. For this account “SaySimple” requires a public end point. For BCT server the URL of this end point is “http://<servername/socialmediaproxy/api/ap/saysimple”. However it is strongly advised not to have BCT server directly connected to the Internet but make use of e.g. a reverse-proxy (as described in “Securing BCT Web Applications” white paper). In that case you can configure (define) your own end point URL to be used by “SaySimple”.

Please contact your NEC representative for additional information.

If a proxy server must be used to send messages to Social Media Providers, see 32 Appendix V – Exchange and Social Media Proxy Settings.

In case of problems with certain social media attachmentents, see 11.3.16 - Social Media Attachment problems.

8.2.5. Phone-based agents

You can allow agents to switch their status in BCT via a (feature) phone. The following agent status can be entered: Logon, Logoff, Ready, Not Ready, Work ready. Login requires the agent to enter a unique PIN code.

On a iS3000, SV8300/SV9300 or SV8500/SV9500 they can do this via:

- dialing an IVR line;
- dialing prefixes;
- programmed function keys on feature phones.

On an AspireX/AspireUX, SV8100/SV9100 or Univerge-3C they can only do this via dialing an IVR line.

See the Login/Logout sections of the PBX configuration chapters how to configure the PBX.

Univerge-3C

When a user centric user with more than one device uses phone based agent dialing via an IVR line, with a configuration key it can be selected which devices related to the user will receive calls (routed/non-routed):

- All devices related to the user having call-offering checked in 3C configuration will receive calls. This is the default setting. Call-offering flags are not affected.
- Only the device which was used by the user to logon via the IVR starter line will receive calls. When agent logon is selected the call-offering flag will be checked for this device, for all other devices call-offering will be unchecked.
  When agent logoff is selected all call-offering flags will be restored to the setting as before logon.

1. Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example. Most likely location: C:\Program Files (x86)\NEC\UCS-Module\Server.
2. Enable / Include:

```
<add key="ChangeCallOfferingOnPhoneLogin" value="True"/>
```

(note that the key might be present in a comment block, so include it outside the comment)

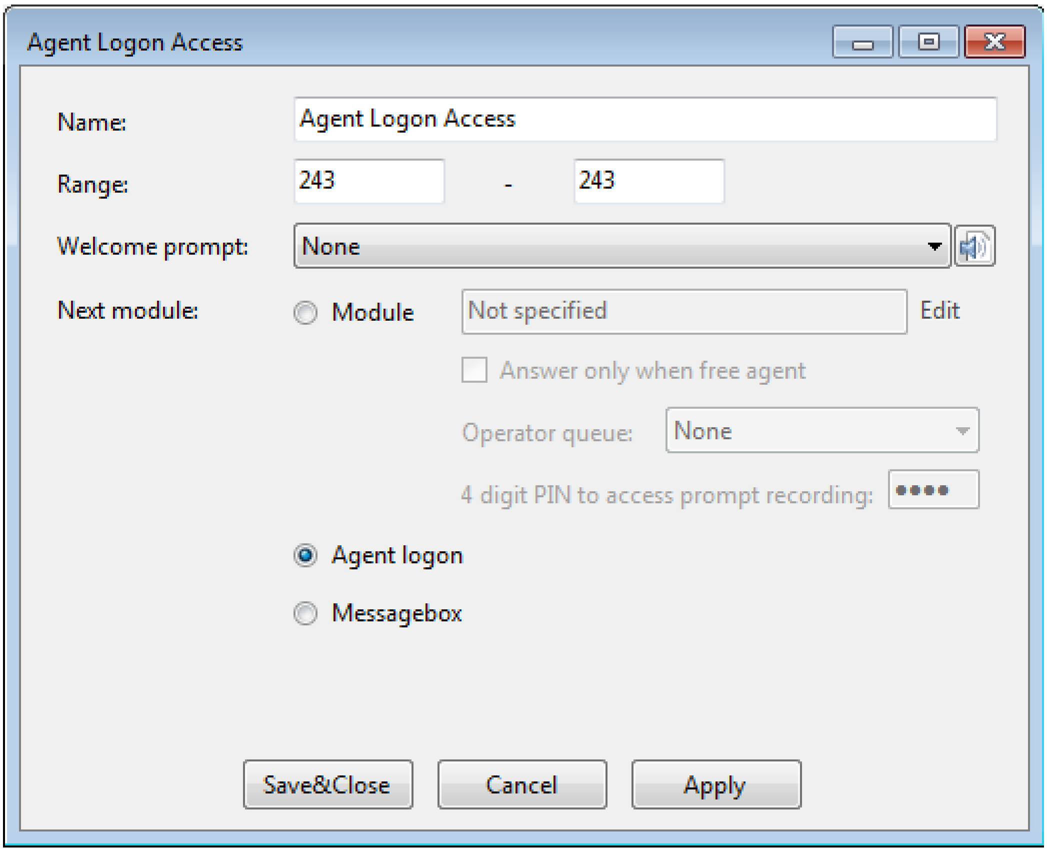
3. Save the file.
4. Restart UCS Runtime

Agent status switching via an IVR line

Phone based agents may switch their status by doing the following:

1. Call the BCT Agent Logon number;
2. When prompted, enter the pin code;
3. Follow the voice prompts;

To configure this feature use the BCT Supervisor Dashboard to create a Starter Line with the radio button “Agent Logon” as next module.



Agent Logon Access

Name: Agent Logon Access

Range: 243 - 243

Welcome prompt: None

Next module: ○ Module Not specified Edit

□ Answer only when free agent

Operator queue: None

4 digit PIN to access prompt recording: ●●●●

● Agent logon

○ Messagebox

Figure 8-42 Agent Logon Starter Line configuration

Phone based agent status switching via function keys

When the agent uses a feature phone and presses the pre-defined function key for agent status switching, by default the text "Agent Status:?" is shown in the default language of the BCT system. The agent can enter the state, terminated with a #.

Note: *It is also possible that the agent uses a feature phone having a pre-defined function key for every status required.*

When the requested state is Logon, a PIN-code is required to enter the requested state. By default, the text "PIN:?" is shown in the default language of the BCT system. The agent enters his PIN-code and terminates with a #. The LED in the function key will change accordingly. The text is generated by BCT.

In case the default language of the BCT system is Japanese, a dedicated function key will be available for each requested agent status. By default, these function keys are mapped to MSF mode codes 128 to 132.

For all other (than Japanese) default languages of the BCT system, the requested agent statuses are mapped to one single function key. Per default the MSF mode code of this function key will be 128.

In both cases, the default MSF codes for agent status function keys may be changed.

The following procedure outlines how to configure the language, e.g. Japanese, for the request texts on the feature phone.

1. Define the “Language to be used by selecting the default language for BCT in the system settings see 8.1.12 Miscellaneous.
   Be aware that on the server the correct regional and language options must be set.

2. When the default MSF mode codes defined cannot be used, change them by the correct mode codes. Below a snapshot of the Phone base agent configuration section of the CTIConfig.xml file is given. Be aware that only the green colored parts may be changed.

```
<PhoneBasedAgentConfiguration>
     <PBX IP="192.168.35.230" Type="SV8300">
       <FunctionKeyData>
          <LogOnKey OaiFunctionCode="128" />
          <LogOffKey OaiFunctionCode="129" />
          <ReadyKey OaiFunctionCode="130" />
          <NotReadyKey OaiFunctionCode="131" />
          <CallTypeKey OaiFunctionCode="132" />
          <CRMKey OaiFunctionCode="133" />
       </FunctionKeyData>
     </ PBX>
     <DisplayData>
        <Language Name="en-US ">
           <DisplayRequestText>
              <AgentStateRequest Text="Agent Status:?" />
              <AgentPinRequest Text="Pin:?" />
              <NotReadyReasonRequest Text="Reason:?" />
              <CallTypeRequest Text="Call Type:?" />
              <MessageRequest Text="Message:?" />
           </DisplayRequestText>
        </Language>
        <Language Name="ja-JP">
           <DisplayRequestText>
              <AgentStateRequest Text="" />
              <AgentPinRequest Text="" />
              <NotReadyReasonRequest Text="" />
              <CallTypeRequest Text="" />
             <MessageRequest Text="" />
           </DisplayRequestText>
        </Language>
        <Language Name="nl-NL">
           <DisplayRequestText>
              <AgentStateRequest Text="Agent toestand:?" />
              <AgentPinRequest Text="Pin code:?" />
              <NotReadyReasonRequest Text="Absentie reden:?" />
              <CallTypeRequest Text="Gespreks info:?" />
              <MessageRequest Text="Bericht:?" />
           </DisplayRequestText>
         </Language>
     </DisplayData>
<PhoneBasedAgentConfiguration>
```

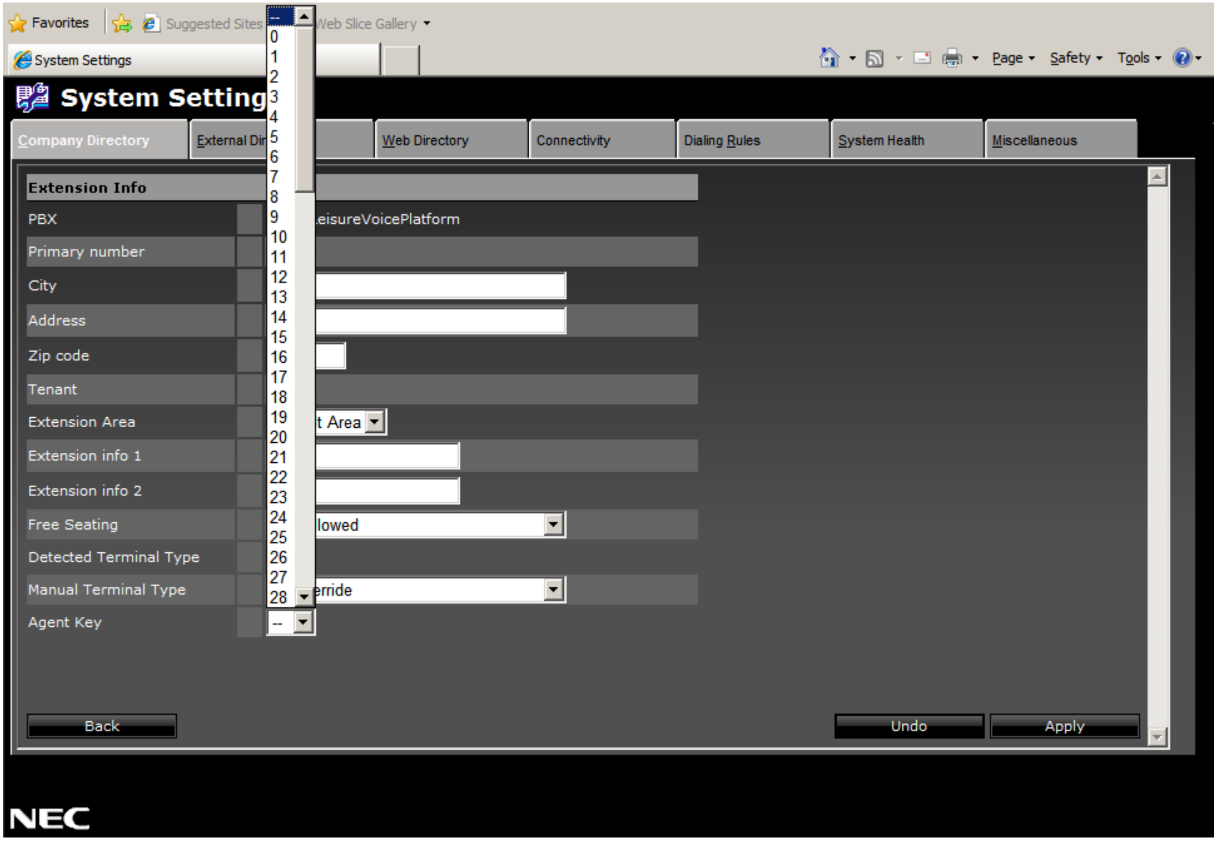
3. Define the Agent Key programmed for Agent Logon:

   - Start the BCT System Settings via Start >All programs >Business ConneCT and login as Administrator.

   - Go to the Company Directory via BCT System Settings.

   - Select the Extension view and enter the extension number of the agent.

   - Select the key number programmed for Agent switching (OAI function key) in the field "Agent Key". See Figure 8-43 Agent Key Configuration



Extension Info

PBX	eisureVoicePlatform
Primary number	
City	
Address	
Zip code	
Tenant	
Extension Area	t Area
Extension info 1	
Extension info 2	
Free Seating	llowed
Detected Terminal Type	
Manual Terminal Type	erride
Agent Key	--

Figure 8-43 Agent Key Configuration

For (all) phone-based agents, you can select whether or not to use automatic answer by BCT. This is done via the Agent settings-tab of the Router Properties window in the BCT Supervisor Dashboard. Please refer to the BCT Administrator Guide, chapter "The Agent Routing Tab" for more information.

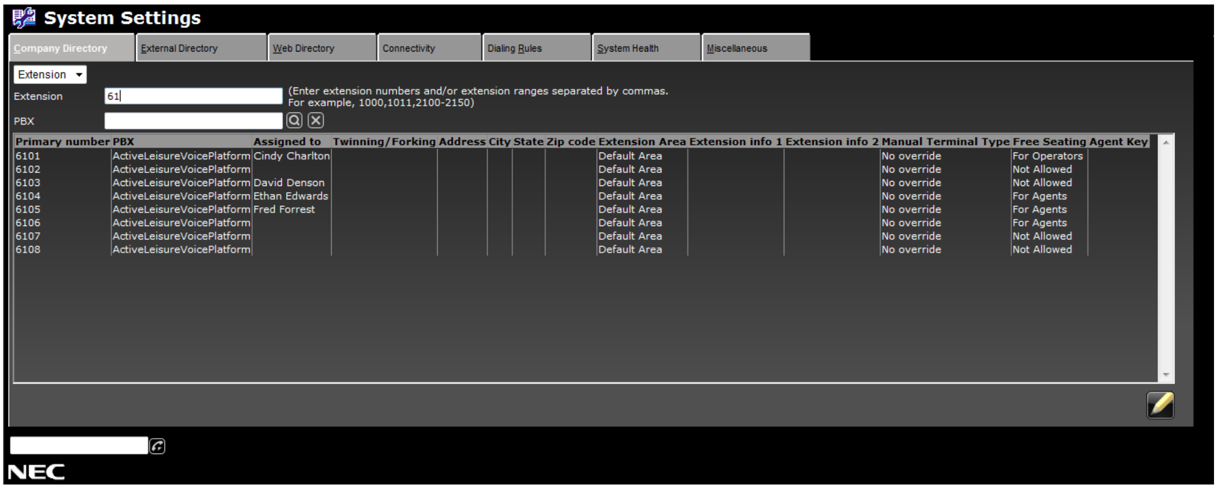
8.2.6. Free seating for agents

Assume there are two workplaces and four agents. It is possible to share these workplaces amongst the four agents using free seating.

Assume the workplaces are equipped with telephones with the numbers 2234 and 2235. The first step is to enable free seating for the extensions 2234 and 2235.

1. Open the “Company directory” tab of the BCT System Settings.

2. Select “Extension” searching and type 223 in the Extension field. See Figure 8-44 Extension search in Company Directory.



Extension

Extension 61

(Enter extension numbers and/or extension ranges separated by commas.
For example, 1000,1011,2100-2150)

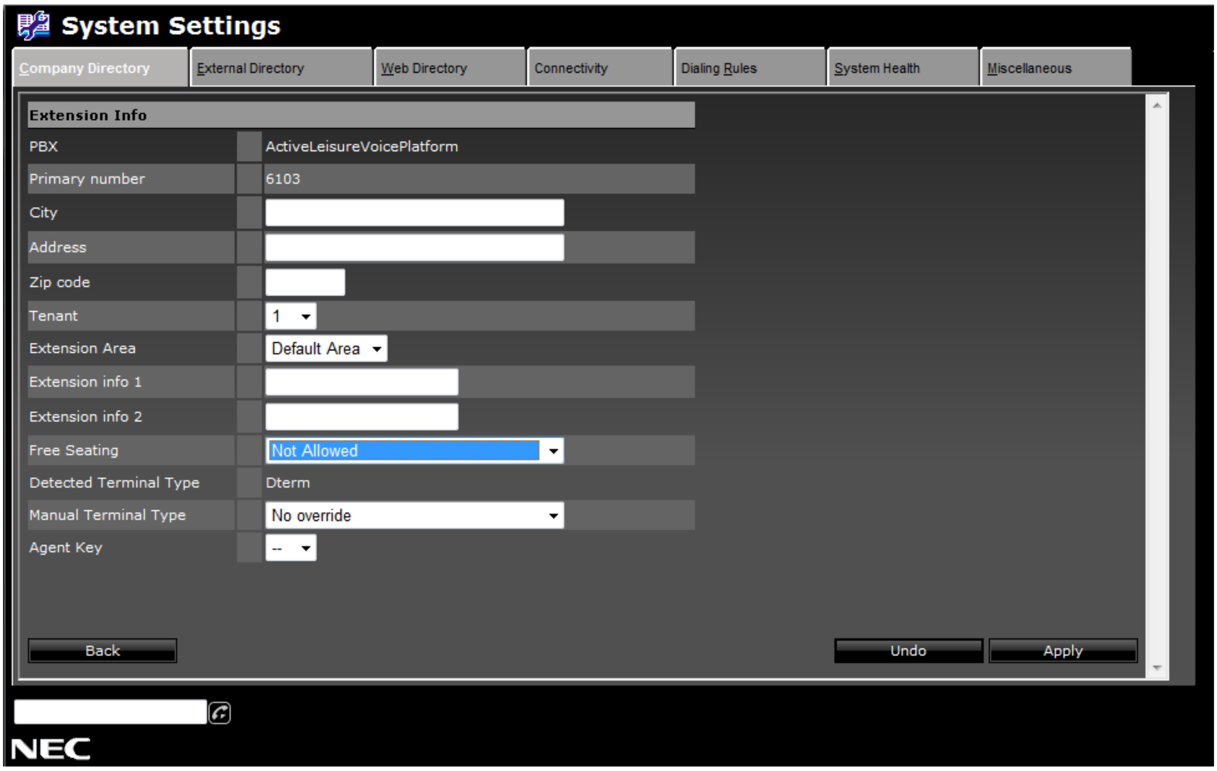
PBX

Primary number	PBX	Assigned to	Twinning/Forking	Address	City	State	Zip code	Extension Area	Extension info 1	Extension info 2	Manual Terminal Type	Free Seating	Agent Key
6101	ActiveLeisureVoicePlatform	Cindy Charlton						Default Area			No override	For Operators	
6102	ActiveLeisureVoicePlatform							Default Area			No override	Not Allowed	
6103	ActiveLeisureVoicePlatform	David Denson						Default Area			No override	Not Allowed	
6104	ActiveLeisureVoicePlatform	Ethan Edwards						Default Area			No override	For Agents	
6105	ActiveLeisureVoicePlatform	Fred Forrest						Default Area			No override	For Agents	
6106	ActiveLeisureVoicePlatform							Default Area			No override	For Agents	
6107	ActiveLeisureVoicePlatform							Default Area			No override	Not Allowed	
6108	ActiveLeisureVoicePlatform							Default Area			No override	Not Allowed	

Figure 8-44 Extension search in Company Directory

3. Now select 2234 and open it with Edit. Open the list in the Free Seating Field, see Figure 8-45 Free seating selection. In this example select “For Agents”.

4. Do the same for extension 2235.

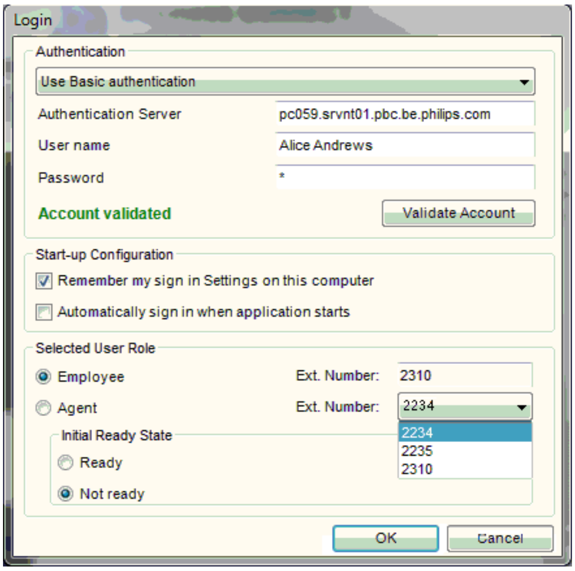


Extension Info	
PBX	ActiveLeisureVoicePlatform
Primary number	6103
City	
Address	
Zip code	
Tenant	1
Extension Area	Default Area
Extension info 1	
Extension info 2	
Free Seating	Not Allowed
Detected Terminal Type	Dterm
Manual Terminal Type	No override
Agent Key	--

Figure 8-45 Free seating selection

5. Verify the result.
Assume we have an agent who wants to use the workplace with telephone 2234. The

selection of the telephone is done during the client logon, see Figure 8-46 Login client with free seating. It is now possible to select 2234 and click **OK**.



Authentication

Use Basic authentication

Authentication Server: pc059.srvnt01.pbc.be.philips.com

User name: Alice Andrews

Password: *

Account validated

Start-up Configuration

☑ Remember my sign in Settings on this computer

□ Automatically sign in when application starts

Selected User Role

● Employee Ext. Number: 2310

○ Agent Ext. Number: 2234

2234
2235
2310

Initial Ready State

○ Ready

● Not ready

Figure 8-46 Login client with free seating

Now the agent can use extension 2234 for agent calls. Extension 2310 still functions as employee extension, also in the presence status.

8.2.7. Configure Agent Idle Time

The basic mode for Call Center routing is on “Longest Idle” agent. A call routed to the agent who was idle for the longest time, compared to the other agents. The Agent Idle Time starts as soon as the last routed call is completed (including ACW time). It is possible to configure the definition of the Agent Idle Time:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRunTime.WinService.exe.config“.

2. Locate the key: AgentIdleWhenNotReady. When True, the Agent Idle Time includes the time when the agent is Not Ready.When False, the Agent Idle Time does not include the time when the agent is Not Ready and the Agent Idle Time is reset to 0 when the Not Ready period ends.
   Default = True.

3. Locate the key: AgentIdleWhenOutgoing. When True, the Agent Idle Time includes the time when the agent is in an outgoing call. When False, the Agent Idle Time does not include the time when the agent is in an outgoing call, and the Agent Idle Time is reset to 0 when the outgoing call ends.
   Default = True.

4. Press button Save to store the value.

5. Restart UCS Runtime service.

8.2.8. Show forwarding destination of users

When logged in as Agent, users can hover over the presence icon of a certain user in the Directory or Groups views and see in the tooltip if that user has forwarding set up or not. By default it is not visible what the forwarding destination is.

However, showing the forwarding destination can be configured:

1. Open the Configuration Manager and select the configuration file C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config".

2. Locate the key the key corresponding to the role we want to have forwarding set up: AgentIncludeFwdDestInPresenceToolTip

3. Change the value to "true"

4. Press button Save to store the value.

5. Then activate the change, reboot the server or restart the "NEC Remoting Service".

8.3. Operator configuration

Note: *If you have configured the system using the Configuration Wizard, you can go straight to section 8.3.5 Announcements in operator queue (optional) and/or 8.3.6 Set the default focus on the talk zone input field (optional).*

Note: *Free seating for operators can be used in the same way as explained for agents. See 8.2.6 Free seating for agents.*

BCT supports concurrent operators, but you can create more operators each with their own login. This way the operator task can be performed by multiple users, but not concurrently. To configure the operators, use the BCT System Settings / Company directory.

The operator can only use an IVR less configuration, but IVR functions can be used. Without media components (voice board or VMP software), prompts and music on hold cannot be played. If these are required and no media component is present in the system, the operator can still be configured as IVR-less. In this case the application will check for a free IVR-line when the prompt needs to be played. If no line is free, the prompt or music will not be played and the application will continue with the routing.

Operators normally run in Pick and Call mode; the operator decides which call to take first. Alternatively the operator can run in Forced Feed mode. In that case the operator cannot select an incoming call, the next call is automatically transferred. This second option is efficient only for dedicated operators. Be aware there is no default priority of external calls over internal calls. The longest waiting call in the Queue will automatically be transferred. When this option is selected the operator becomes a Contact Center agent.
Note: A parked call in 'Forced feed' mode of the operator immediately bounces back to the operator if the line is free. So the Park Queue becomes useless.
This can be solved by creating a separate Operator Park Router identical to the Operator router but the activation delay set to 9999.

To set up the operator Call Flow, you must:

1. Create Operator & Operator Group

2. Create Operator Router

3. Create Operator Starter and Starter Lines

4. Create Operator Night Extension

You do these tasks via the BCT Supervisor Dashboard in configurator mode as **Administrator**.

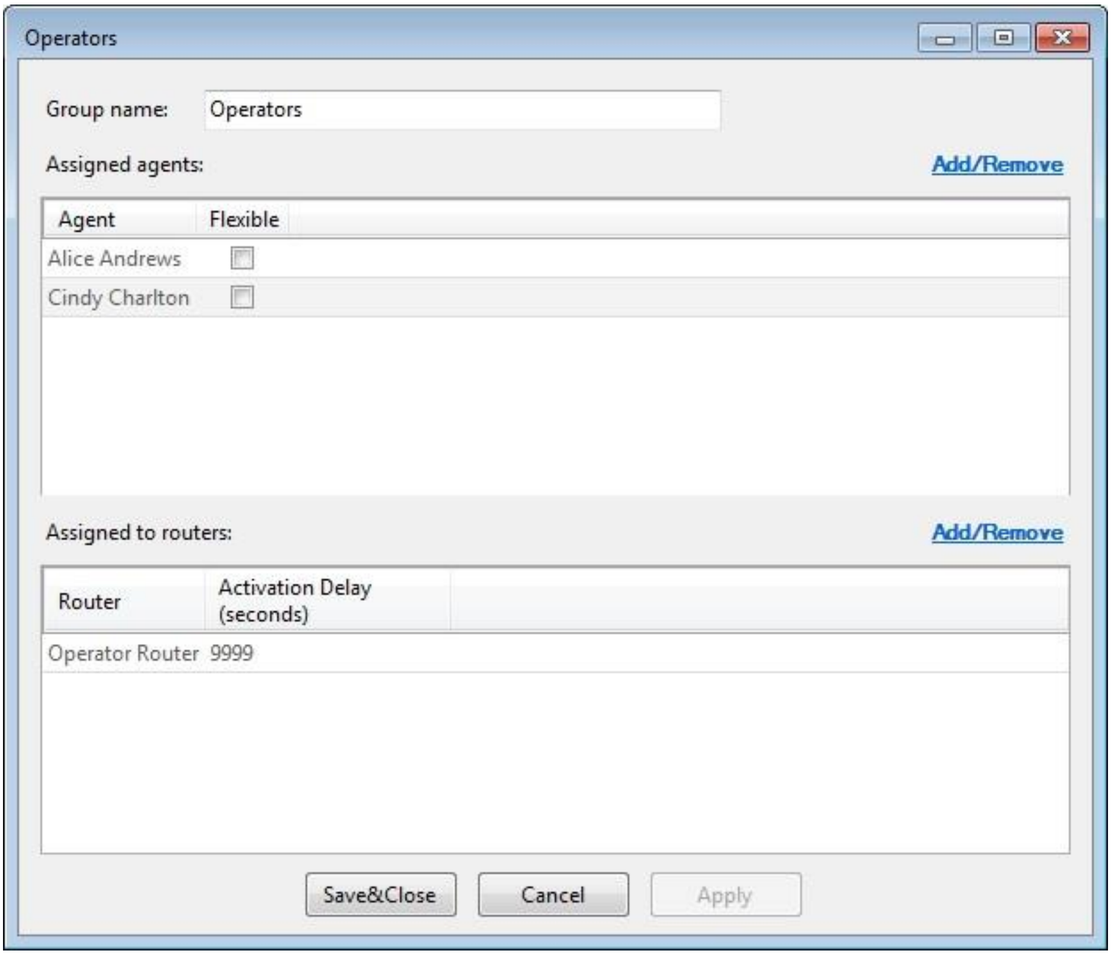
8.3.1. Create an Operator and Operator Group

1. Create operators via the BCT System Settings.

2. If you have defined the operator group already in BCT Supervisor Dashboard (see step 3), then you can assign the operator to the group from the BCT System Settings.

3. The operators are part of a special group that is going to be used for routing purposes; groups are located in the **Resources** area of the explorer view of BCT Supervisor Dashboard. Select **Groups** and all created groups will be displayed in the main window. If you select a group, all assigned agents/operators to this group will be listed. Use Add/Remove to assign or remove agents from the group.

4. To create a new group, select **New** from the toolbar. A new group is now created. Right click the new group and enter the properties window. Change the name of the group and assign the operator to this group via the Assign Agents button. The Assign to Routers button can be used later to assign a Call Flow for this group.



Group name: Operators

Assigned agents:

Agent	Flexible
Alice Andrews	□
Cindy Charlton	□

Assigned to routers:

Router	Activation Delay (seconds)
Operator Router	9999

Figure 8-47 Operator assistance group properties

After configuration is complete, this should show the agents with BCT operator access and the operator router (see next section).

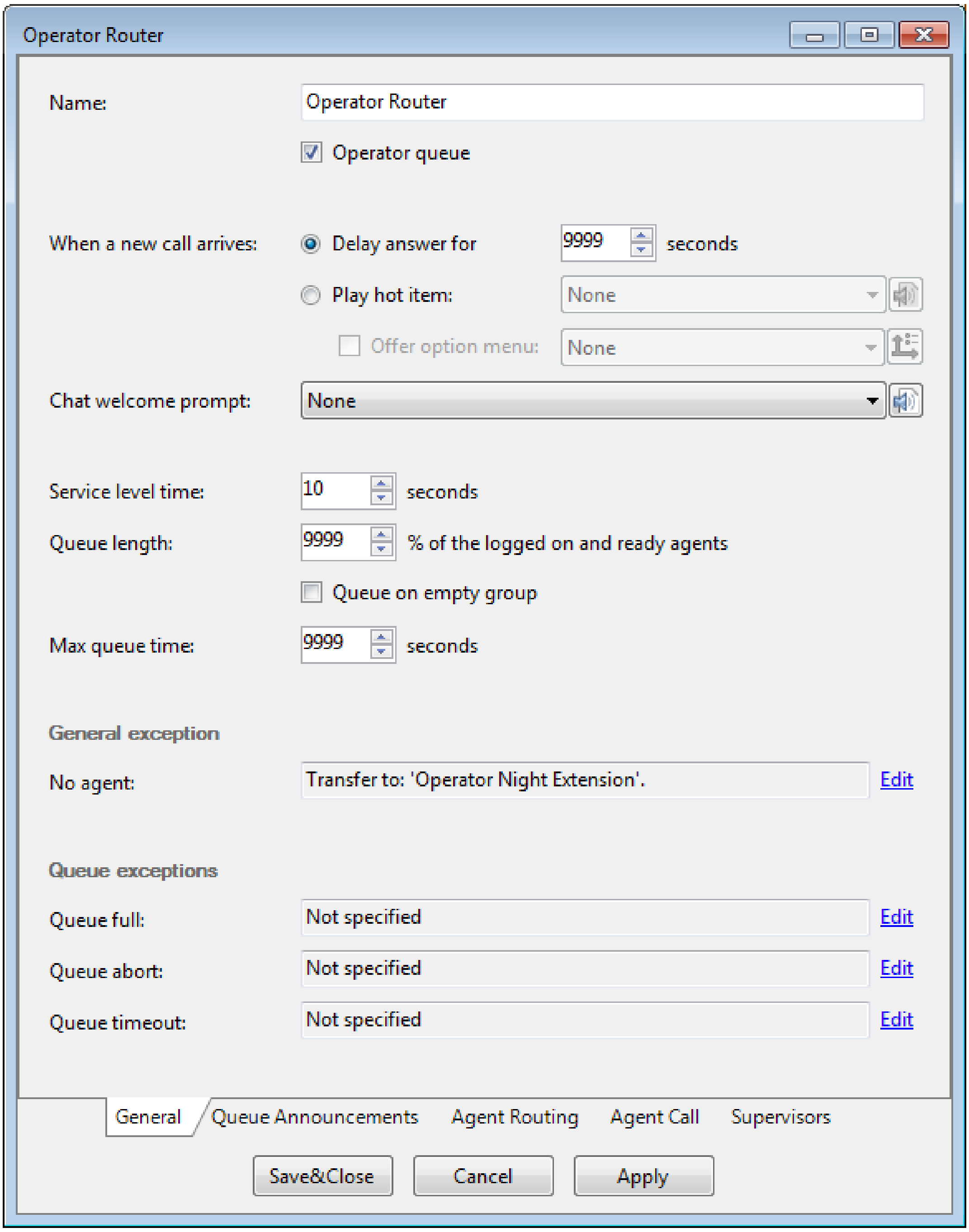
8.3.2. Create Operator Router

The Call Flow for the operator consists of two basic elements, routers and Starter Lines. A router gives the direction what to do with an incoming call. Also Queue parameters and exceptions on the normal operation state are determined by the router characteristics. The operator mode, “Pick and Call” or “Forced Feed” is also determined by the router properties.

To create a router, use the following procedure:

1. Routers are located in the **Modules** area of the explorer view. Select **Router** and all created routers will be displayed in the main window. To create a new router, select **New** from the

toolbar. A new router is now created.



Operator Router

Name: Operator Router

☑ Operator queue

When a new call arrives: ● Delay answer for 9999 seconds

○ Play hot item: None

□ Offer option menu: None

Chat welcome prompt: None

Service level time: 10 seconds

Queue length: 9999 % of the logged on and ready agents

□ Queue on empty group

Max queue time: 9999 seconds

General exception

No agent: Transfer to: 'Operator Night Extension'. Edit

Queue exceptions

Queue full: Not specified Edit

Queue abort: Not specified Edit

Queue timeout: Not specified Edit

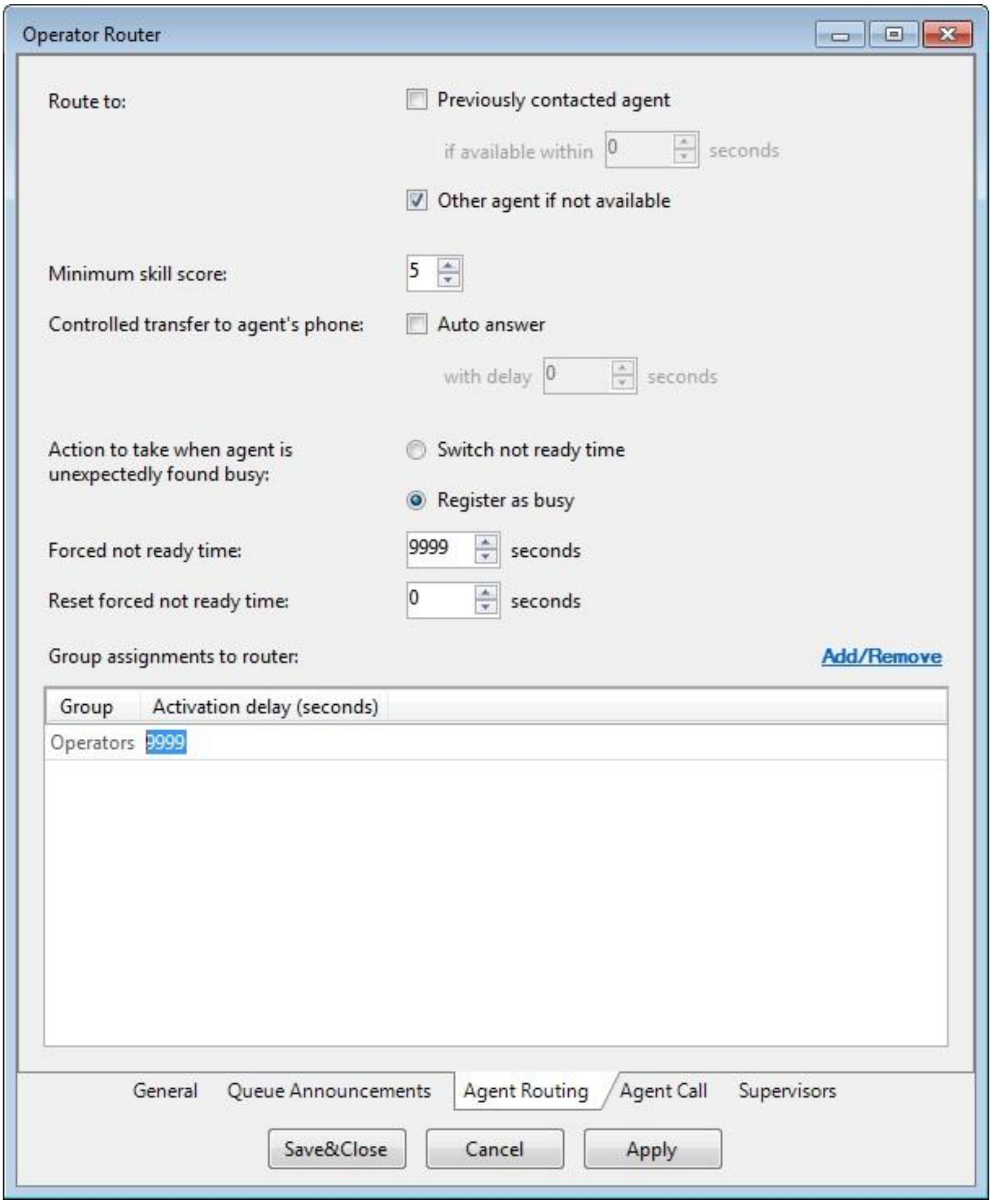
Figure 8-48 Router properties for operator call flow

2. Edit the new router:

- Change the name of the router to for instance Operator router;
- Set the 'Maximum queue time' to maximum 9999 seconds, operators do not have an overflow destination;
- Set the 'After call work time' to zero, the operator does not use this Contact Center feature;
- Set the ‘Service Level Time’ to the appropriate level, 10 seconds (3 rings) for ‘Pick and Call’ mode and 5 seconds for ‘Forced Feed’ mode are quite reasonable;

- Set ‘Forced not ready time' to maximum 9999 seconds, operator should never be logged off by the system;
- Set 'Number of queue positions as % of logged on and ready agents' to maximum 9999%;
- Check the Operator Queue checkbox;

The created router needs to be assigned to the operator group. Click on the **Agent Routing** tab in the Router properties. Click on the **Add/Remove** button. Select the Operator group and move it to the router area by clicking the arrow button. Then Close the application by pressing Done.



Operator Router

Route to: □ Previously contacted agent

if available within 0 seconds

☑ Other agent if not available

Minimum skill score: 5

Controlled transfer to agent's phone: □ Auto answer

with delay 0 seconds

Action to take when agent is unexpectedly found busy: ○ Switch not ready time ● Register as busy

Forced not ready time: 9999 seconds

Reset forced not ready time: 0 seconds

Group assignments to router: Add/Remove

Group	Activation delay (seconds)
Operators	9999

Figure 8-49 Assign the operator router to the operator group

3. The choice for the operator mode ‘Pick and Call’ or ‘Forced Feed’ can be made by creating an activation delay for the selected operator group, using the same **Agent Routing** tab. If the delay is set to zero, new calls automatically go to an unoccupied operator (Forced Feed). If the delay is set to maximum (9999 seconds) the call stays in the Queue until the operator manually selects the call. Pick and Call mode is preferred.

Note that if you do use Forced Feed, the operator cannot use the “Autoanswer of selected queued calls” option because the BCT client will not show this option.

8.3.3. Create Operator Starter and Starter lines

A starter links a call to the router. By creating different access points or Starter Lines, the system shows users the origin of a call. The operator needs four Starter Lines:

- External calls to the general access number;
- Operator assistance (internal) calls;
- Fallback calls, unsuccessful calls that fallback to the operator;
- Park position, calls that were parked by the operator.

To create the starter and Starter Line follow the following procedure:

1. In the **Callflow** area of the explorer view, select **Starter.** You see a single Starter Line. Select the properties of this Starter Line, and for **Mode of operation**, select Normal.

2. To create a new Starter Line, select **New** from the toolbar.

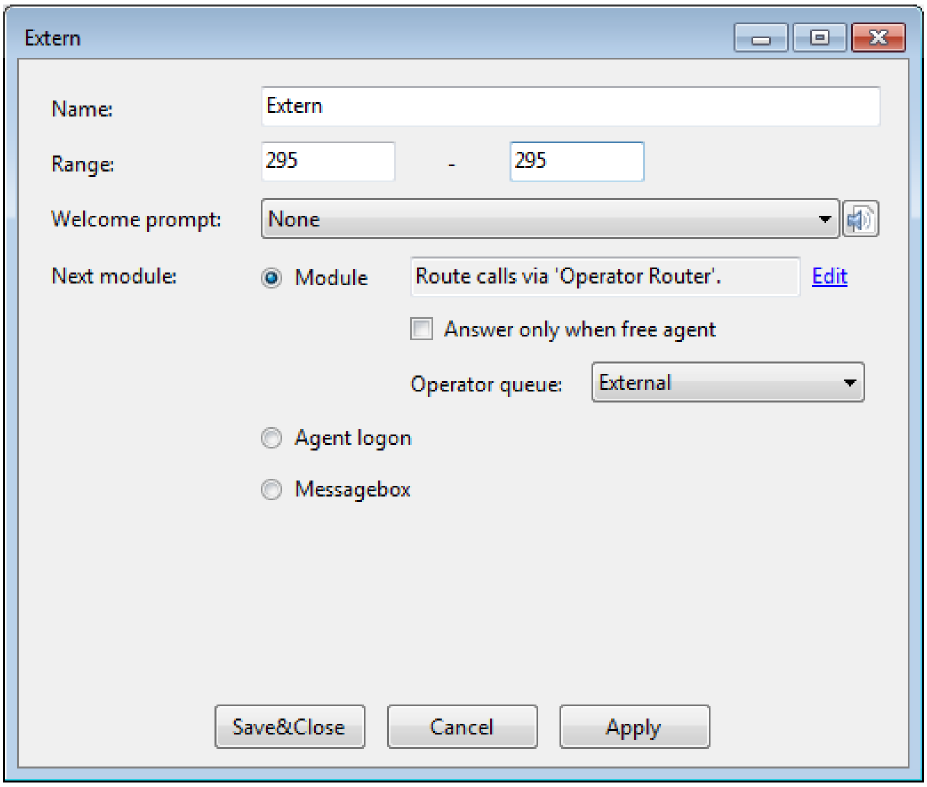
3. Fill in the name of the new starter and the station number (DNR) of this line, i.e. 9 for Operator Assistance;

4. Select the welcome prompt by clicking the icon next to the welcome prompt field, prompts can only be played if an IVR line is free;

5. Select Next modules to link the Starter Line to a router. Select **router** as module and the just created **Operator router** as router. If using ‘Force Feed’ mode, also select the priority level of calls via this Starter Line, 1 is the lowest priority. Calls with a higher priority will be answered first. This way external calls can be handled more quickly than internal calls. Click **OK**.

Note: *Do not link the starter to e.g. a clock first and then the clock to a router. Otherwise a call will not return to the operator after Camp on Busy time-out.*

6. Repeat the procedure for all four operator Starter Lines.



Extern

Name: Extern

Range: 295 - 295

Welcome prompt: None

Next module: ● Module Route calls via 'Operator Router'. Edit

□ Answer only when free agent

Operator queue: External

○ Agent logon

○ Messagebox

Figure 8-50 Properties of an operator starter line, this starter line routes via the Operator Router.

8.3.4. Create Operator Night Extension

When the last operator closes BCT in the evening, the calls should be redirected to the Operator Night Extension.

1. Create Operator Night extension transfer. This extension is used to transfer calls when no operators are present. Transfers are located in the **Callflow** area of the explorer window. To create a new transfer, select **New** from the toolbar.

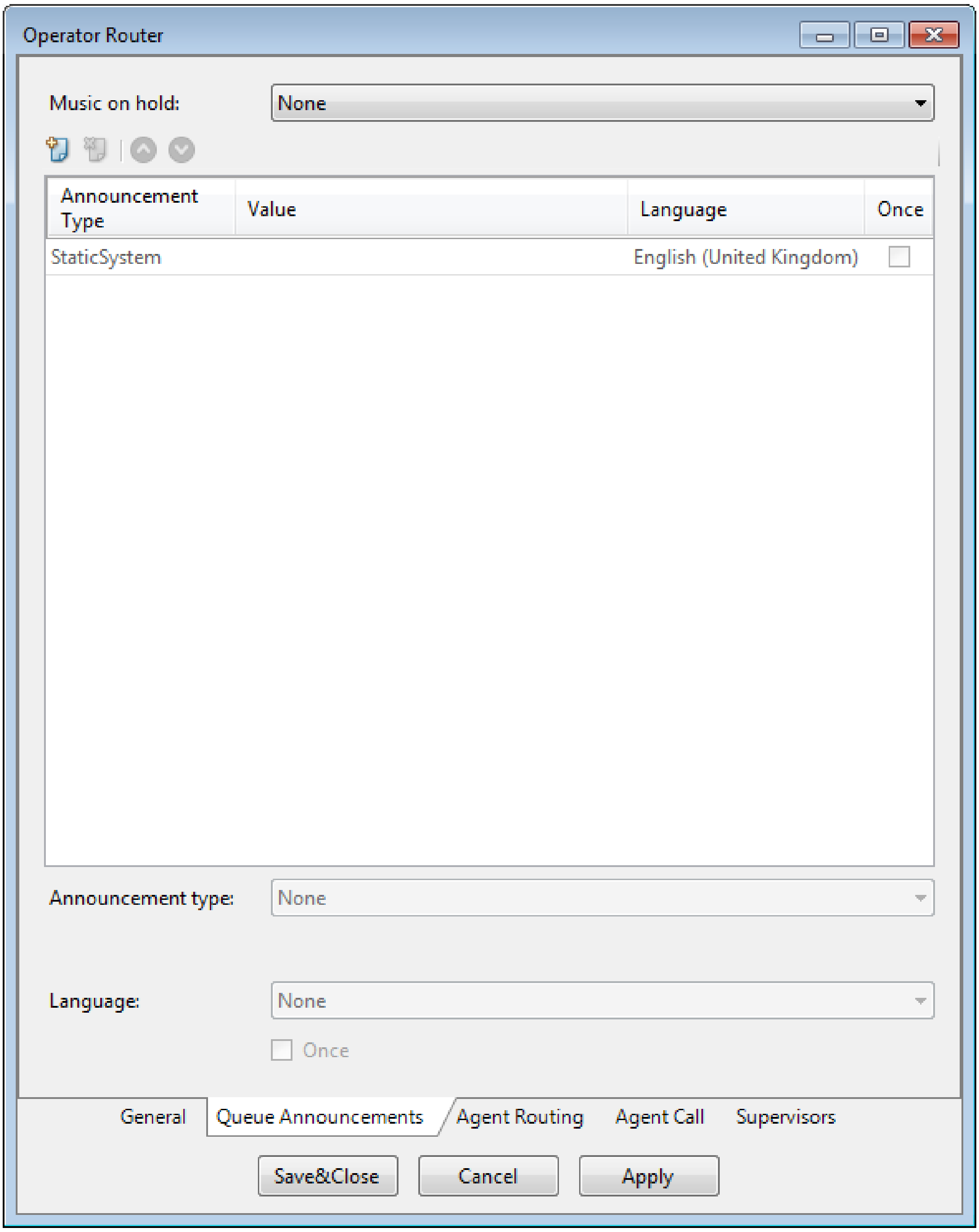
- Fill in the name of the transfer, i.e. Operator Night Extension;
- Enter the destination number in the digits to dial;
- Select 'Blind' type of Transfer.

2. Go Back to the routers via **Callflow > Router** and select the operator router. Select Exceptions and add the operator Night Extension as General Exception 'No Agent'

- Select Transfer as module;
- Select the Operator Night Extension as transfer destination;
- Press OK.

8.3.5. Announcements in operator queue (optional)

If you want callers to hear announcements while they wait, you can specify this in the Caller Settings tab of the Router Properties:



Music on hold: None

Announcement Type	Value	Language	Once
StaticSystem		English (United Kingdom)	□

Announcement type: None

Language: None

□ Once

Figure 8-51 Announcements in operator queue

Note: *If you set a Delay Answer time, then that delay will also apply to the Queue Messages.*

8.3.6. Set the default focus on the talk zone input field (optional)

By default the focus is on the Directory input field. If your operators require the focus on the Talk field, you can change the default focus as follows:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common\NEC\Serivce\RemotingService.WinService.exe.config”.

2. Locate the key: isStealFocusEnabled

3. Change the value to “false”

4. Press button Save to store the value.

5. Restart the Remoting Service (or the whole system).

6. Restart the client to activate the change.

8.3.7. Change the “Parked blinking timer”

By default when a call is parked for more than 30 seconds, the Park Queue icon

icon starts blinking .

This time can be changed.

1. Open the Configuration Manager and select the configuration file C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config”.

2. Locate the key: ParkedCallNotificationTime

3. Change the value to the required time in seconds.

4. Press button Save to store the value.

5. Then activate the change, reboot the server or restart the “NEC Remoting Service”.

8.3.8. Change the “Queue Ringtone Delay timer”

When the operator ends call and there are still calls in the Queue, the Ringtone (A ringtone has to be selected) starts after 3 seconds (Default).

This time can be changed.

1. Open the Configuration Manager and select the configuration file C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config”.

2. Locate the key: QueueRingToneDelay

3. Change the value to the required time in seconds.

4. Press button Save to store the value.

5. Then activate the change, reboot the server or restart the “NEC Remoting Service”.

8.3.9. Show forwarding destination of users

When logged in as Operator, users can hover over the presence icon of a certain user in the Directory or Groups views and see in the tooltip if that user has forwarding set up or not. By default it is not visible what the forwarding destination is.

However, showing the forwarding destination can be configured:

6. Open the Configuration Manager and select the configuration file C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config".

7. Locate the key the key corresponding to the role we want to have forwarding set up: OperatorIncludeFwdDestInPresenceToolTip

8. Change the value to "true"

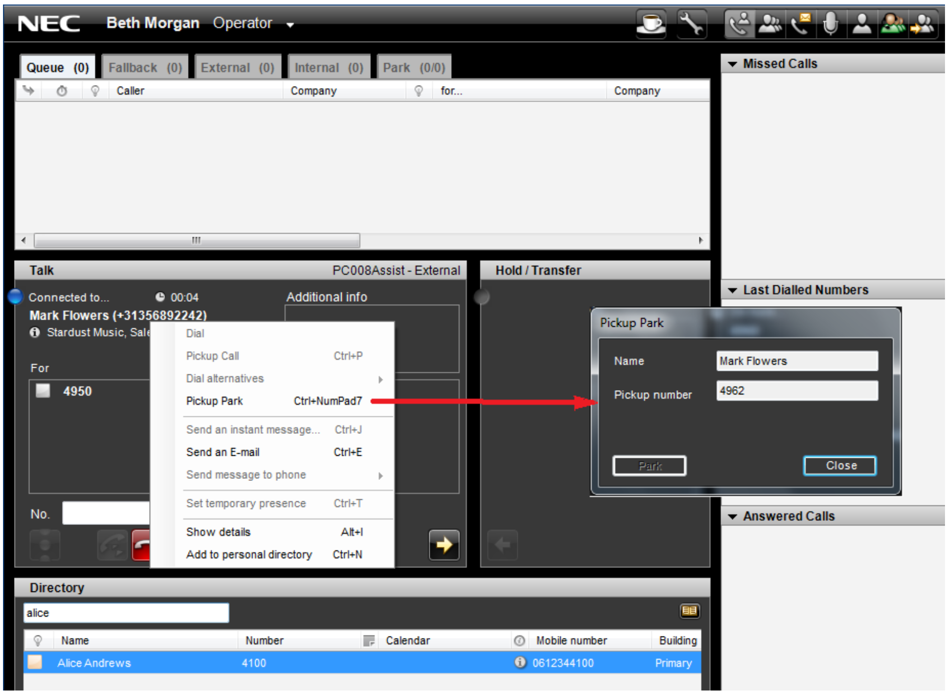
9. Press button Save to store the value.

10. Then activate the change, reboot the server or restart the "NEC Remoting Service".

8.3.10. Create System Call Park configuration

System Call Park (also called Pickup Park) is a feature to allow an operator to park a call on a System Call Park position and let another user pickup the caller from this park position.

The operator performs this action by pressing the Right mouse button on the caller in the call pane and selecting "Pickup Park" item from the context menu. A "Pickup Park" popup window appears, to let the operator confirm the System call park action by pressing the "Park" button. At that moment the Pickup number is filled in by the system with a free System Call Park position.



Mark Flowers (+31356892242)
Stardust Music, Sale

4950

Name: Mark Flowers
Pickup number: 4962

alice

Name	Number	Calendar	Mobile number	Building
Alice Andrews	4100		0612344100	Primary

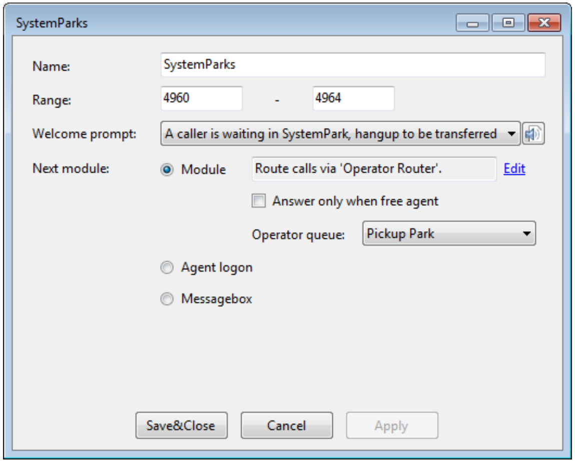
The operator now contacts the intended user to inform about the waiting caller and the pickup number to dial to retrieve the caller (e.g. by broadcasting or instant messaging). The user then calls this pickup number, hears a dedicated prompt and is automatically transferred to the waiting caller.

To configure the System Call Park functionality use the following procedure:

1. Add the routing points for the System Call Park positions as assigned routing points in the BCT Supervisor Dashboard, see 8.1.6.9 Routing Points.

2. Create a dedicated application prompt for the user calling the pickup number, for instance "A caller is waiting in the System park, hang up to be transferred".

3. Create a Starter Line with the first System Call Park Routing point in the “From:” field and the last System Call Park Routing point in the “To:” field. Select the dedicated prompt in the “Welcome prompt” field. Select the Operator Router as Next module and select Pickup Park in the Operator queue type Queue drop down box. After completion the configuration an operator can use the System Call Park functionality upon login.



Name: SystemParks

Range: 4960 - 4964

Welcome prompt: A caller is waiting in SystemPark, hangup to be transferred

Next module: ● Module Route calls via 'Operator Router'. Edit

□ Answer only when free agent

Operator queue: Pickup Park

○ Agent logon

○ Messagebox

8.3.11. Disable showing call-related photos in the operator talk-zone

To disable showing call-related photos in the operator talk-zone follow the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config“.
2. Locate the key: isShowPhotosInOperatorModeEnabled
3. Change the value to false.
4. Press button Save to store the value.
5. Activate the change by reboot the server or restart the “NEC Remoting Service”.

8.3.12. Customize email message for missed calls

When the operator is in a call and the called party cannot be reached, the operator can send an email to the called party by pressing F3.

By default, the subject and the body of the email have a predefined content in the language of the operator.

To customize the content of the email:

1. Copy the file “C:\NEC\Data Files\Template Files\EmailToCalledPartyTemplate.xml” to a new file “C:\NEC\Data Files\Template Files\EmailToCalledParty.xml”.
2. Edit “C:\NEC\Data Files\Template Files\EmailToCalledParty.xml”, adapt the content of EmailSubject and EmailBody, and save the file.

Next time an operator presses F3 the email will be composed as defined in the file.

This function is general for all operators and the content of the file will not be translated.

3. When the file is deleted, the old functionality will become available again.

8.4. Contact Center configuration settings

8.4.1. Show forwarding destination of users

When logged in as Employee, users can hover over the presence icon of a certain user in the Directory or Groups views and see in the tooltip if that user has forwarding set up or not. By default it is not visible what the forwarding destination is.

However, showing the forwarding destination can be configured:

1. Open the Configuration Manager and select the configuration file C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config".

2. Locate the key the key corresponding to the role we want to have forwarding set up: or EmployeeIncludeFwdDestInPresenceToolTip

3. Change the value to "true"

4. Press button Save to store the value.

5. Then activate the change, reboot the server or restart the "NEC Remoting Service".

8.4.2. Show additional information to Agents for outbound campaign calls

The data of the next (standard) columns in the dialing list will be shown on the desktop client of an agent in case a call is received from an outbound user defined service.

- Telephone and Name (both shown at the 'Connected to' data of the client)
- Personal ID (has its own display-location within the detailed information)
- Description (this and next are shown at the specific area for detailed information).
- Skill1 and skill2
- Language
- Email Address

The data displayed within the detailed information by default contains 4 lines, the 1st containing the description, the 2nd containing the skills, the 3rd containing the language and the 4th containing the email-address.

As described in BCT Administrator Guide (Outbound Service Dialing List tab), additional data can be added to a dialing list entry by importing a file containing 1 to 6 additional columns named "Additional1" up to and including "Additional6". This additional data can be displayed by defining 1 to 4 configuration keys (AgentAdditionalLine1 .. AgentAdditionalLine4).

1. Open the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common files\NEC\Services\RemotingService.WinService.exe.config"

2. Locate the key: AgentAdditionalLine1 (or 2, 3 or 4)

3. Change the value to contain a formattable string (explained below)

4. Press button Save to store the value.

The contents of AgentAdditionalLine1 will be used to replace the first line of the detailed information, etc.

Example: the formattable AgentAdditionalLine2: “Appointment date: {1}, time: {5}” will display “Appointment date: 22-6-2019, time: 10:30” on the 2nd line of the additional panel, where format item {1} is replaced with the contents of the Additional1 column (of the dialing list) and format item {5} is replaced with the contents of the Additional5 column. Note that the format items {1} .. {6} correspond to the Additional1 .. Additional6 of the dialing list. Format item {0} is a special case and will be replaced with the Description column of the dialing list.
Each of the 4 default lines of the detailed information can be replaced separately. In case one of the AgentAdditionalLines contains the value “#original#”, or is not configured, the default contents (description, skill, language or email) will be displayed. In case a line needs to be suppressed, configure an AgentAdditionalLine with an empty value “”. This leads to display a corresponding empty line in the detailed information.

8.4.3. How to disable "Route Calls From Routing Point”

When routing calls from a routing point the destination phone shows the correct calling party.
To get the same behavior as BCT 9.0 or earlier (routing calls from VMP line), this feature can be disabled.

To disable the "Route Calls From Routing Point"-feature system-wide, execute the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRuntime.WinService.exe.config”

2. Locate the key: RouteCallsFromRoutingPoint

3. Change the default value (True) by False if you want the same behavior as BCT 9.0 or earlier.

4. Press button Save to store the value.

8.4.4. Allow Agents to set forward for direct calls (SV9100-TAPI only)

When forwarding immediate is set, an agent is set to not ready and when an agent is switched ready forwarding immediate is reset.
With the "Ignore Forwarding For Agent State"-feature active Agents can set forward for direct calls. This key is only valid for SV9100-TAPI.

To enable the "Ignore Forwarding For Agent State"-feature system-wide, execute the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRuntime.WinService.exe.config”

2. Locate the key: IgnoreForwardingForAgentState

3. Change the default value (False) by True

4. Press button Save to store the value.

Note: With this feature routed calls go always via a Routing Point.

8.4.5. Single or daily timing for Not Ready Reasons

The default behavior for time-limits for Not Ready reasons implies that the used time for each Not Ready reason is kept per agent and per day. This behavior can be changed so that the time-limit is applied for each Not Ready period separately. A configured coffee break of 15 minutes by default implies that an agent can have e.g. 3 coffee breaks of 5 minutes before his time expires. By changing the setting named “DisableDailyNotReadyTimeLimits” this behavior is changed and each time an agent takes a coffee break the timer is re-started at 15 minutes again.

To disable the daily behavior, execute the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRuntime.WinService.exe.config”

2. Locate the key: DisableDailyNotReadyTimeLimits

3. Change the default value (False) by True if you want non-daily behavior.

4. Press button Save to store the value.

8.4.6. How to disable “Out Of Router Transfer As Direct Call”

When an agent transfers a routed call to another agent outside the router, the routed call becomes a direct call for reporting (default).
To get a routed call with contact data and the same reporting as BCT 10.10 or earlier, this feature can be disabled.

To disable the "Out Of Router Transfer As Direct Call "-feature system-wide, execute the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\NEC\UCS-Module\Server\UCSRuntime.WinService.exe.config”

2. Locate the key: OutOfRouterTransferAsDirectCall

3. Change the default value (False) by True if you want non-daily behavior.

4. Press button Save to store the value.

8.5. Extension and User Directory configuration

8.5.1. Extension Configuration (Company Directory)

Extension data can be added or changed via the BCT System Settings. The BCT System Settings is a web application. To access Extension data do the following:

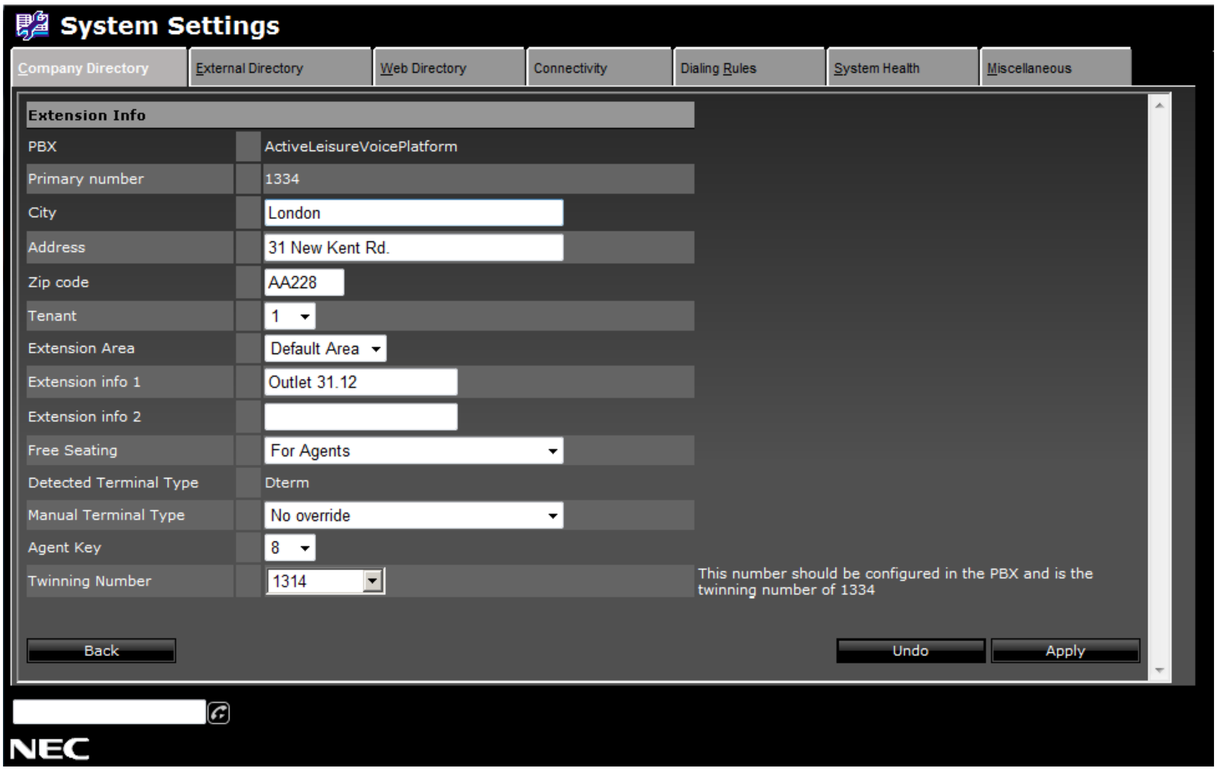
1. Select Start>Program files (x86)>Business ConneCT> BCT System Settings.
   Or, go to http://<servername>/ca/ca.aspx.

2. Login as **Administrator** (default no password).

3. Select the **Company Directory** tab. This administrator interface looks almost the same as the window of a user login in to Directory Browser. However, when you login as administrator you can also enter data.

4. Select **Extension** from the element selection box in the top left part of the Company Directory window.

5. Select an extension and click the Edit button. Note that if you click on a name, you go to the Employee edit window.



Extension Info	
PBX	ActiveLeisureVoicePlatform
Primary number	1334
City	London
Address	31 New Kent Rd.
Zip code	AA228
Tenant	1
Extension Area	Default Area
Extension info 1	Outlet 31.12
Extension info 2	
Free Seating	For Agents
Detected Terminal Type	Dterm
Manual Terminal Type	No override
Agent Key	8
Twinning Number	1314

This number should be configured in the PBX and is the twinning number of 1334

Figure 8-52 Company Directory configuration window

Each synchronized extension is entered in the database with a number of attributes:

- PBX: the PBX the extension belongs to.
- Primary Number: the extension number.
- City: the city where the extension resides (optional).
- Address: the address where the extension resides (optional).
- Zip code: the zip code where the extension resides (optional).
- Tenant: the tenant number (not relevant for iS3000).
- Extension Area: If you have more areas, you may have to select another area than the Default Area for this extension. See 8.1.11 Dialing Rules and 18 Appendix H – DIALING RULES AND NUMBER CONVERSION.
- Extension info 1: additional info field (optional).
- Extension Info 2: additional info field (optional).
- These two fields can be used for example to indicate the physical location of the terminal.

- Free seating: determines whether this extension can be used for free seated operators/agents or operators and agents. Default setting is the setting “not allowed”.

- Detected Terminal Type: the type of terminal as detected by the PBX Synchronization process.

- Manual Terminal Type: a manual override option to change the detected terminal. This may be required if the Terminal Type cannot be determined exactly by the PBX Synchronization process. Manual override is not allowed for each terminal type, but only for specific Terminal Types in specific PBXs.
  This option is for instance required when IP DECT terminals are used, these can be detected as Dterm-IPs.

- Agent key: in case of a SV8300/SV9300 or SV8500/SV9500 enter the OAI function key number for terminal Mode Set Facility (MSF). It enables an OAI function key for phone based agents. Note that you also need to program this under a Dterm key in the PBX programming. See also section 8.2.5 Phone-based agents

- Twinning number: In case of IS3000, you may use Twinning. You need to define for the extension on which the user logs in, that there is a Twinning extension number. In the example in
  Figure 8-52 Company Directory configuration window the user logs in on extension 1334, and has a Twinning number 1314.
  Note that this must also be configured in the PBX (see 4.5.4.2 Twinning).
  For SV9100-TAPI this is called forking (Dual ring). You can define for the extension on which the user logs in, that there is a Forking extension number.

- User Name For Display: If an extension is assigned to more than one user, you can select which user you want to have displayed as opposite party of calls, and in lists (like e.g. the Call Log). In that case a dropdown list is shown from which you can select the username to display.

Note: *When silent charging is activated for the IP DECT terminal, the terminal cannot be detected when placed in the docking station. The default terminal type is Dterm-IP in this case. Therefore change the Terminal Type manually for all IP DECT terminals.*

Note: *By removing the Voicemail role from an existing user, all old Voicemail and greeting messages will be removed. An exception to this rule is when the user has no Agent/ Operator/ Employee role assigned, in which case the Administrator can choose to keep the messages. This exception is useful when changing the extension of a user.*

8.5.1.1. Set terminal type

Under normal conditions the terminal types are set automatically after PBX Synchronization to the right values. Should there however be a mismatch between assigned terminal type and actual terminal type, then this has to be adjusted manually.

It is important to assign the right terminal type to an extension, otherwise the terminal cannot be controlled correctly from the BCT Client.

You can edit multiple extensions in one-go.

1. Login to BCT System Settings as ‘Administrator’.

2. Select **Extension** from the element selection box

3. Enter your selection in the Extension field.
   Enter extension numbers and/or extension ranges separated by commas. For example: “2010-2020, 2400”.

4. Press the **Edit** button (✎).

5. The Edit page will appear. Make the required selection from the **Manual Terminal Type** drop down list. Selecting a Terminal type from the dropdown list should be interpreted as “act as this type of terminal”.

6. Press **Apply** to save the changes.

Notes on Manual Terminal Type selection:

- IP DECT Terminal
  A DECT terminal with “Silent Charging On” and placed in the loader is not registered in the PBX. When BCT is synchronized with the PBX it is not possible to detect the terminal type in that situation. So in case of “Silent Charging On” it is recommended to use the Manual Terminal Override function and choose terminal type “IPDect”

- Support for answering DECT phones (IPDECT G266 / G566 / G966 / I766 / I766x /G277 / G577) via BCT is supported for iS3000/Sip@Net and 3C (Sphericall). For 3C, the terminal type needs to be manually overridden, use the Manual Terminal Override function and choose terminal type “IPDect G/Ix66 series”.

- SIP Phone on SV8500/SV9500
  A not-registered SIP Phone is not recognized when BCT is synchronized with the SV8500/SV9500. Use Manual Terminal Override function and choose terminal type “SIP” in this case.

- The Manual Terminal Type dropdown list is PBX dependent and not all types are shown.

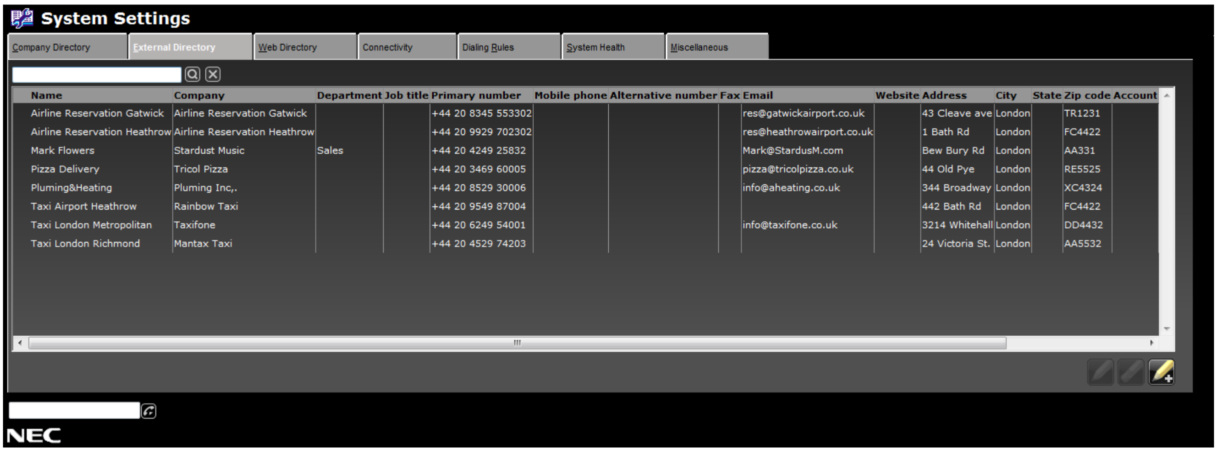
- The Polycom / DT700 / DT800 / DT900 type are SIP phones with SIP controlled answer.

- A Softphone is usually a SIP phone.

The detected terminal type also depends on programmed function keys (see PBX specific section).

8.5.2. External Directory configuration

External contacts can be entered in the database via the following procedure:



Name	Company	Department	Job title	Primary number	Mobile phone	Alternative number	Fax	Email	Website	Address	City	State	Zip code	Account
Airline Reservation Gatwick	Airline Reservation Gatwick			+44 20 8345 553302				res@gatwickairport.co.uk		43 Cleave ave	London		TR1231	
Airline Reservation Heathrow	Airline Reservation Heathrow			+44 20 9929 702302				res@heathrowairport.co.uk		1 Bath Rd	London		FC4422	
Mark Flowers	Stardust Music	Sales		+44 20 4249 25832				Mark@StardusM.com		Bew Bury Rd	London		AA331	
Pizza Delivery	Tricol Pizza			+44 20 3469 60005				pizza@tricolpizza.co.uk		44 Old Pye	London		RE5525	
Pluming&Heating	Pluming Inc,.			+44 20 8529 30006				info@aheating.co.uk		344 Broadway	London		XC4324	
Taxi Airport Heathrow	Rainbow Taxi			+44 20 9549 87004						442 Bath Rd	London		FC4422	
Taxi London Metropolitan	Taxifone			+44 20 6249 54001				info@taxifone.co.uk		3214 Whitehall	London		DD4432	
Taxi London Richmond	Mantax Taxi			+44 20 4529 74203						24 Victoria St.	London		AA5532	

Figure 8-53 External directory configuration window

Steps:

1. Login to BCT as Administrator
2. Select the External Directory tab
3. Add an external number by pressing 'New'.
   Note: You can assign a company name to the external contact via an editable dropdown box. You can select an existing company; or add a new company name by selection '—Add New Company' and change this field into the new company name. You can also change a selected company name by editing it. But pay attention to the warning, so you're sure this is what you intendent to do: "**Attention: This action will rename the company name for all related contacts. If you wanted to rename the company name only for this contact you should select - Add New Company and edit that.**"

As with the company directory, you can import the external directory using a CSV file.
Note: CSV files must contain field enclosed in quotemarks, separated by commas, like "field","field".

8.5.2.1. Searching in the External Directory

External contacts have only one name field, no separate first, middle and last name field.
Per default, the search algorithm uses the searchstring that you enter and placed a wildcard in front of and behind it. This means that it will always find a match if the searchstring is present anywhere in a name field.

However, in case your External Directory is very large (e.g. larger than 20.000 entries), it is advised to prevent the search taking too much time. You can configure the search algorithm to only put a wildcard behind the searchstring. In this case, if the directory contains "John Smith" and your searchstring is "John", the search algorithm will search for "John%" and find it. But if your searchstring is "Smith", the search algorithm searches for "Smith%" and it won't find it.

To configure this:

- Open the Configuration Manager and select the configuration file" folder C:\Program Files (x86)\Common Files\NEC\Services\DirectoryService.WinService.exe.config".

- Locate the key: UseWildcardSearchByDefault
- Change the value to “false”
- Press button Save to store the value.
- Restart the Directory Service or restart the system

8.5.2.2. Company Privacy for the External Directory

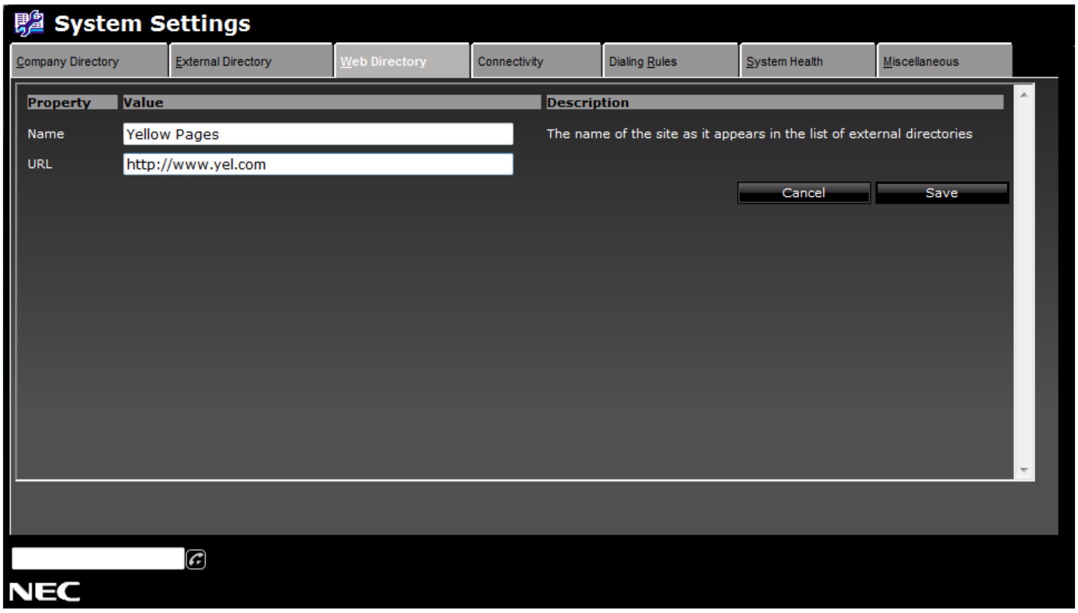
When Company Privacy is also to be applied to the External Directory (then users cannot see contact data of external contact related to other companies), then the company name must be put into one of the user defined fields of the External Directory (Info1..Info4).

To make this operation, you need to configure this as follows:

- Add a key to the configuration file “RemotingService.WinService.exe.config” in the folder C:\Program Files (x86)\Common Files\NEC\Services: "CompanyPrivacyForExternalDirectoryConfiguration" and the value must be 1..4.
- Add a key to the configuration file "web.config" in the folder C:\Inetpub/wwwroot/DirectoryBrowser: "CompanyPrivacyForExternalDirectoryConfiguration" and the value must be 1..4.

8.5.3. Web Directory configuration

By Web Directories of BCT are meant: any web based directories available on the internet. The Web Directory Configuration creates a hyperlink to this internet phone directory and makes them available to end users in the BCT client application.



Property	Value	Description
Name	Yellow Pages	The name of the site as it appears in the list of external directories
URL	http://www.yel.com	

Figure 8-54 Web directory configuration window

Steps:

1. Login to BCT System Settings as ‘Administrator’.

2. Select the Web Directory tab

3. Select **New**.

4. Enter a name and the corresponding URL, then click **Save**.

8.5.4. DECT Directory Access configuration

DECT terminal users can access the Company (or Central) Directory to search for an entry, look at the presence information and set up a call. To allow this, you must modify the following file: DataAccess.dll.config configuration.

1. Open the file DataAccess.dll.config, with the Notepad editor for example.

Default location: C:\Program Files (x86)\Common Files\NEC\Services directory. (When the system was upgraded the location path is C:\Program Files (x86)\Common Files\Philips\Services)

2. Find the key “directory.service.presence.algorithm” and set its value to “BCTOnly”.

3. Save the file.

4. Reboot the server.

Optionally, it is possible to configure whether a Central Directory Access search looks into the Company Directory, the External Directory, or both. To do that:

1. Open the Configuration Manager and select the configuration file” C:\Program Files (x86)\Common Files\NEC\Services\DirectoryService.WinService.exe.config".

2. Locate the key: CDA_CentralDirectory_1

3. Default value is "CompanyDirectory". To include the External Directory in the search, change it to "CompanyDirectory, ExternalDirectory". To limit the searches to External Directory only, change it to "ExternalDirectory".

4. Press button Save to store the value.

5. Restart the Directory Service or restart the system

On certain versions of IP DECT software/DECT terminals, it is possible to configure multi-directory access. This enables DECT handset users to activate multiple “central directories” they can search in.

Each directory is identified by a “directory number” which is part of its name, for example “*Central directory 2*”. The behavior of searches in each directory can be configured individually within BCT.

To configure multi-directory access behavior within BCT:

1. Open the file "DirectoryService.WinService.exe.config" in the folder C:\Program Files (x86)\Common Files\NEC\Services.

2. Add one or more keys in the configuration file, as follows:

```
<add key="CDA_CentralDirectory_2" value="CompanyDirectory"/>
<add key="CDA_CentralDirectory_3" value="ExternalDirectory"/>
```

The number in the key name identifies the “directory number” which is being accessed from the DECT handset.

3. Save the file

4. Restart the Directory Service or restart the system

Note: *Central Directory Access must be enabled/configured within IP DECT. For more information on how to do this, refer to IP DECT Tools and Maintenance Manual.*

8.5.5. Company Directory (User) configuration

After Synchronization (see 8.1.5 Connection to PBX), the company directory is filled with all extensions of all PBX units connected to the BCT server via the CTI link. The company directory is not only used as source for BCT, it is also used as database for user administration of BCT applications.

The administration of BCT is web based. Username is “Administrator”, no Password (default). The administrator can login by using one of the following methods:

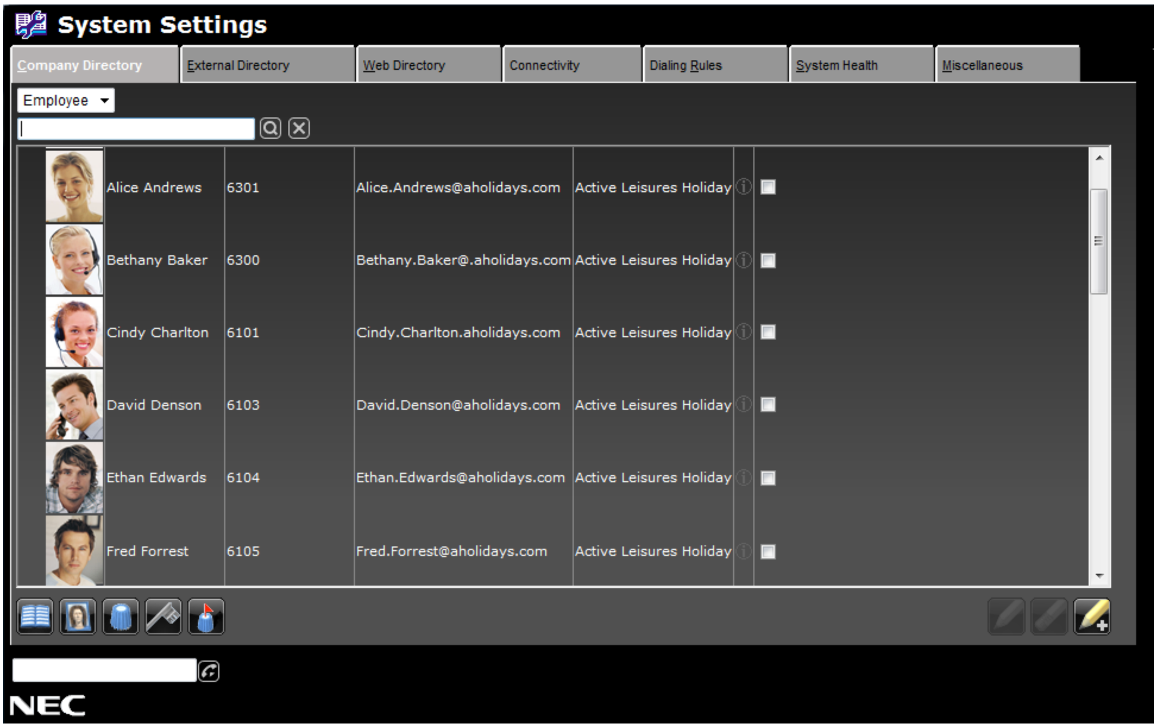
- at: http://<servername>/ca/ca.aspx or
- select Start>Program files (x86)>Business ConneCT> BCT System Settings or
- right-click the “Business ConneCT Status” tray icon and select System Settings. See Figure 11-1 System Health taskbar icon and right mouse menu on BCT server

Steps:

1. Login to BCT as **Administrator** (default no password). The first login from a new PC will trigger a download of client components. Accept the download and press OK

Note: *Localhost is not allowed as <servername>, IP address is.*

2. Select the **Company Directory** window. This administrator interface looks almost the same as the window of a user login in to Directory Browser, you can search the database with names of employees already entered etc. However, when you login as administrator you can also enter data.



Alice Andrews	6301	Alice.Andrews@aholidays.com	Active Leisures Holiday
Bethany Baker	6300	Bethany.Baker@.aholidays.com	Active Leisures Holiday
Cindy Charlton	6101	Cindy.Charlton.aholidays.com	Active Leisures Holiday
David Denson	6103	David.Denson@aholidays.com	Active Leisures Holiday
Ethan Edwards	6104	Ethan.Edwards@aholidays.com	Active Leisures Holiday
Fred Forrest	6105	Fred.Forrest@aholidays.com	Active Leisures Holiday

Figure 8-55 Company directory (User) configuration

The top part of the Company Directory UI shows the following fields:

- The element selection drop-down list, where you can select either Employee, Hierarchy or Extension data. Select **Extension** to see if the data is entered automatically via the Synchronization process via the CTI link.

- The search field(s) can be used to enter search criteria to search the database.

- The search button will search the database.

- The clear button clears the search field.

The middle part of the screen is where the information is displayed.

On the bottom of the screen six buttons can be found to configure the appearance of the electronic phone book. In principle all users can choose their own search and result criteria, the administrator decides what fields they can choose from and what the default criteria are. From left to right:

- The 'Directory Browser' button gives access to the electronic phone book.
- The 'Personal Details button' is used to change the personal data of the user that is logged in. Since you are logged on as Administrator these are the details of the administrator.
- The 'Configuration' button allows you to change the appearance of the search fields and results. Every user has the option to do this.
  - The fields as added in the 'Search on' section are scanned by the browser to find the text string the end-user invoked.

· The fields as added in the 'Find as result' section are returned to the end-user’s browser.

· The 'Combine Search Fields' box is used to offer only one field in the Company Directory for defining a text string to search for.

- The 'Import' button allows you to import users from an Excel sheet, the template is provided via the download link.

The 'Export' button allows you to export users to an Excel sheet. All fields in the table are exported.

- The 'Protection' button allows you to restrict the number of fields available to the user to search on or find as result.

- The 'Default Config' button allows you to choose the default settings for the users.
You can set the default fields to search on, the default fields as added in the 'Find as result' section that are returned to the end-user’s browser, the default fields shown in the reveal details.
Upto 4 additional fields for the Desktop Client internal directory can be added. Each added field can be configured to be handled as text, phonenumber, url or email. When configured as phonenumber, email or url it becomes clickable in the internal directory of the Desktop Client and when clicking on it the appropriate click action is executed (phonenumber is dialed, email is started when email client is installed, and url is shown in web browser).
Warning: No validation on the content of these additional fields is performed. Changing the type e.g. from phonenumber to url will handle the content of this field as url. So if the content was e.g. 1000 then clicking on this field will try to start a browser with url 1000 but will fail.
If Job Title is configured as additional field, the Desktop Client internal directory will also show the Job Title from the External Directory. If User defined field 1 is configured, the Info 1 from the External Directory will be shown. Same for User defined field 2 (Info 2) and User defined field 3 (Info 3).

It is possible to enter alternative names for any of the "User defined fields n" fields, and thus also overrule any translation. To do that:

- Open the Configuration Manager and select the configuration file ‘C:\Inetpub\wwwroot\Directory Browser\web.config’.
- Locate the key : DB_TXT_eEV_userDefined_1 (this is the "User defined field 1" field)
- Fill the value with the desired name, for example "Home address"
- Press button Save to store the value.

In the System Setting page these "User defined field n" fields names will be replaced by the names you have assigned. You can use these fields also in the Full Directory and include them in any possible search / result option.

Note: *These fields of the company directory can be imported / exported, but there the original name will always be used.*

- The ‘Edit’ button becomes active when you select an item in the list.

- The ‘Delete’ button becomes active when you select one or more items in the list.
- The ‘New’ button allows you to add an entry.

On the bottom of the screen you also see a search and dial field. The administrator user interface is an extended BCT user interface. The normal users cannot change the company directory however.

Note: *To delete an entry from a list (employees, extension, PBXs, etc…), you either mark the required checkboxes or select a single entry (by clicking on the row). However, if checkboxes are checked, this will overrule the selected deletion and only the checked entries are deleted!*

8.5.6. Importing users

Note: *If you have imported users after the Configuration Wizard started up the Directory Browser, you can skip this section.*

Note: *If you use UNIVERGE 3C as PBX, adding users by importing them is not possible, as the Active Directory is considered to be the source for users. However, it is possible to update information of existing users in BCT through import. Information brought from 3C can only be updated in BCT if the PBX is configured to allow it.*

It is possible to import names from an external source into the directory, using CSV files. The following procedure must be used:

1. Login to BCT System Settings as ‘Administrator’.

2. Click on the **Import** button. Make sure that when importing names into the company directory the view is set to Employee.

3. Click the text: **Download Full UNICODE Template CSV** or **Download Minimal Template CSV**. As with the company directory, you can import the external directory using a CSV file. Note: CSV files must contain field enclosed in quotemarks, separated by commas, like "field","field".

4. Select **Save as**, this action will save the default template in CSV format. This template can be used to import users.

The template file must be UTF8 or Unicode format, and it must be filled in correctly.
The first line contains the fieldnames of the Employee table. This is the table the names are loaded into. **Do not change these field names**. The ‘LastName’, ‘CompanyName’ and ‘Extension’ fields are mandatory. The following fields can be filled for each user:

- pbxID: only applicable in multi-pbx environments.
- extension;
- firstName;
- middleName: only if applicable
- lastName;

- email;
- LyncUri (Skype for Business URI);
  When this column is left out in the csv file and email is present and filled in then during import the LyncUri (when not yet set) will be set to 'sip:' + email.
- division: the 2nd level of the hierarchy
- department: the lowest level of the hierarchy
- alternateNumber: the alternative number for this user
- companyname: the top level of the hierarchy
- PBC_LoginName: the user name used for *Basic Authentication*, if not supplied the combination of first and lastname will be entered. This entry must be unique. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.
- PBC_NTLogin: the user name used for *Integrated Windows Authentication*. This is the domain login name of the user, including the domain used. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.
- OfficeUser: to create a BCT user for this entry (value 1) or just an entry in the Company Directory (value 0)
- Presence: to enable (value 1) or disable (value 0) presence settings

When the complete hierarchy information is entered this import automatically creates the company's hierarchy. **If not supplied, the entries will all go to the default hierarchy**.

5. Save the file as Unicode csv file.
6. Upload the thus created CSV file using the 'Browse' and 'Upload buttons.
7. Use the **Back** button to see the results in the company directory

Note: *To see mappings between Company import list and items displayed on the BCT client, see chapter 13 Appendix C – DIRECTORY IMPORT AND EXPORT MAPPING*

Repeated import

If you are repeating the import of users into the Company Directory, then BCT will prevent creating double entries, as follows:

- If BCT recognizes a UniqueID (created in a previous export) then it will update the entry rather than insert a new entry.
- If BCT finds that the Lastname + Firstname + Extension is identical to an existing entry, then it will also update that entry.

WARNING: *An exported file (containing users with uniqueIDs) may only be used for import on the same system where it was exported! (in other words it can only be imported in the database that still contains the same unique id that were exported) .*

8.5.7. Directory Import Formatter

The Directory Import Formatter is used to validate a CSV file having a BCT readable format which can be used for import via the Directory Import feature of BCT.

This function is available on the BCT server via Start/Programs/Business Connect/Tools.

It can also be found on the BCT product DVD as tool (Business ConneCT Resources\Configuration Support\Directory Import Formatter folder), so it can be used on another PC than the BCT server

Creating or using a CSV file.

With menu option File -> New, a Personal, Company or External directory import file can be created. With menu option File -> Open a CSV file can be selected which must be converted to a BCT readable format. Assumed is that the CSV file starts with a header line, followed with data lines.

It is also possible to export data from BCT to a CSV file, in this way you can modify the data with the tool and import this again in BCT.

There is a default mapping of names in the header line to column names, but this can be customized when providing a mapping file. A warning is given when the mapping file is not found and the default is used. The format of the mapping file is in the first line the names to be matched in the CSV file and in the second line the BCT field names.

When fields of the header line are recognized, the name of the column is set, when the column is “Ignored” it is not recognized and a field can be selected from the dropdown selection. All "Ignored" columns will not be part of the saved file.

Editing data

When New or Open is done, there is a possibility to enter or modify the data. Via menu option Edit, Cut, Paste, Find and Replace, Find Errors functions are made available.

During entering or modifying, data checks are performed if all required fields are according to the requirements of the specific fields. On errors, the cell with the error will have a red color and a red indication is displayed at the beginning of the line, the tooltip on the error indication will provide more information. The "Esc" button can be used to undo the last changes and to get rid of the error.

Creating a file

The File -> Save As option gives the possibility to save the data in a BCT readable format.

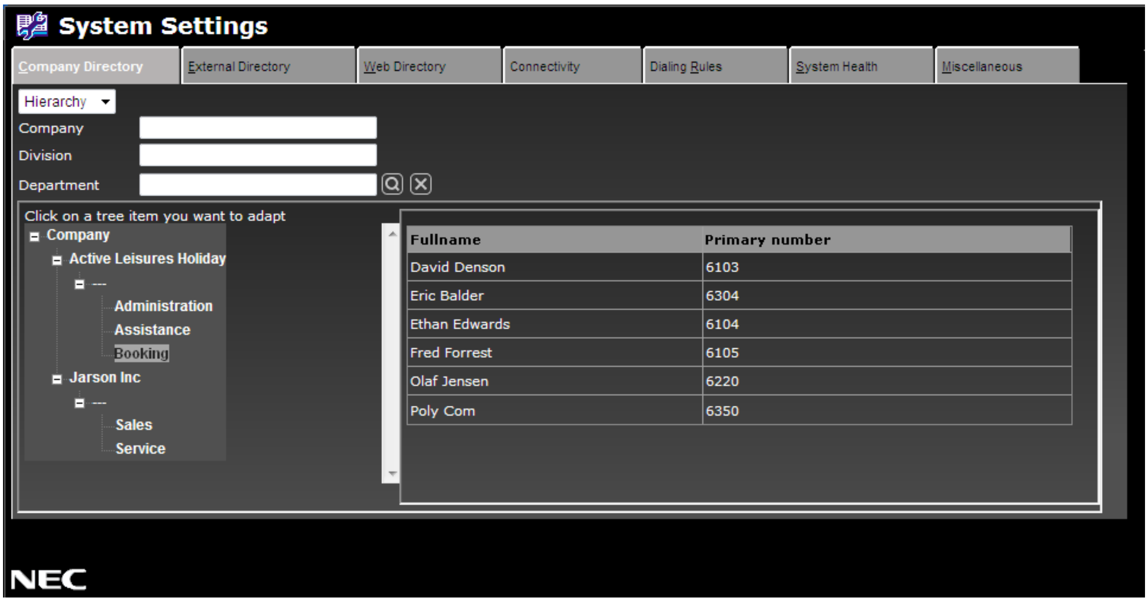
The most common way to use this tool is:

1. Have a data file from excel in CSV format.
2. Open this file with the Directory Import Formatted
3. Check if all required data is available
4. Save this file
5. Import the saved file

8.5.8. Manually create the hierarchy of the customer

1. Login to BCT System Settings as ‘Administrator’.
2. Select **Hierarchy** from the element selection box
3. Click in the tree on the left on company level.
4. Enter the new company name in the field on the right and press **Save**
5. Expand in the tree on the left on the new company’s division level.
6. Enter the new division names in the field on the right and press **Save**
7. Expand in the tree on the left on the new company’s department level.
8. Enter the new department names in the field on the right and press **Save**

At the department level all users belonging to that department are shown in the right pane. If you click on a user, the edit screen for that user will be opened. After editing, return to the previous screen. See Figure 8-56 Company Directory Hierarchy.



Click on a tree item you want to adapt

Fullname	Primary number
David Denson	6103
Eric Balder	6304
Ethan Edwards	6104
Fred Forrest	6105
Olaf Jensen	6220
Poly Com	6350

Figure 8-56 Company Directory Hierarchy

8.5.9. Export

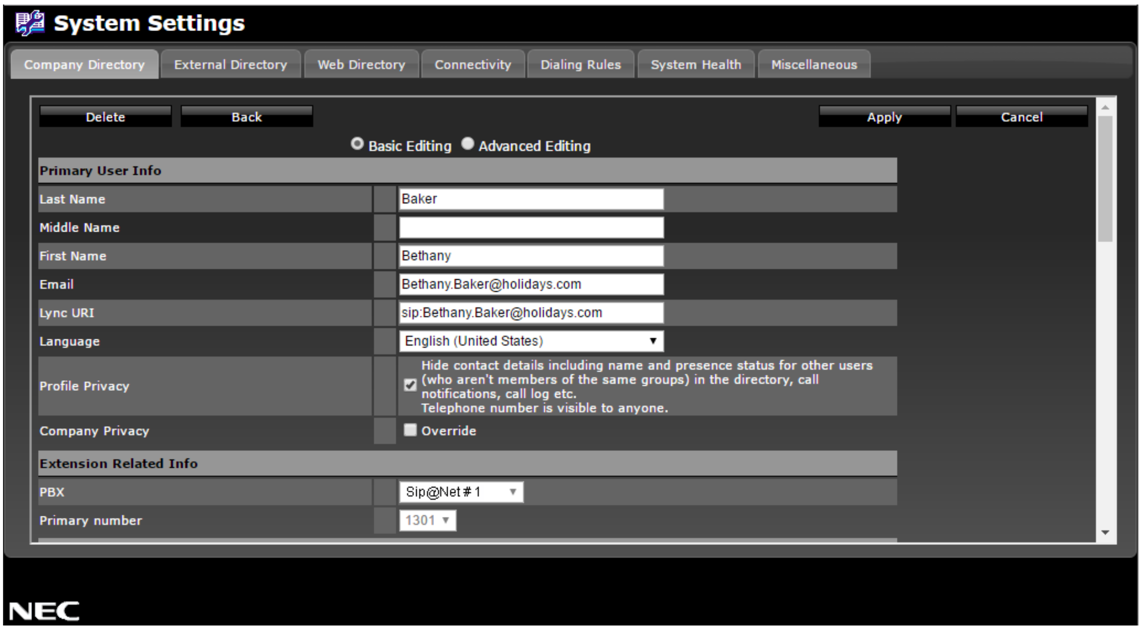
It is possible to export Company directory and external directory data to a file.

With this export file modifications to existing user can be made without creating duplicated users.

8.5.10. Manually create a BCT user

1. Login to BCT System Settings as ‘Administrator’.
2. Select **Employee** from the element selection box.
3. Press the **New** button.

4. Enter the primary user information of the user in the appropriate fields.



● Basic Editing ○ Advanced Editing

Primary User Info	
Last Name	Baker
Middle Name	
First Name	Bethany
Email	Bethany.Baker@holidays.com
Lyncs URI	sip:Bethany.Baker@holidays.com
Language	English (United States) ▾
Profile Privacy	☑ Hide contact details including name and presence status for other users (who aren't members of the same groups) in the directory, call notifications, call log etc. Telephone number is visible to anyone.
Company Privacy	□ Override
Extension Related Info	
PBX	Sip@Net # 1 ▾
Primary number	1301 ▾

Figure 8-57 Company Directory - Edit User part 1

First Name, Middle Name, Last Name: In case you have switched on "Search on alternative names" in System Settings / Miscellaneous (see 8.1.12 Miscellaneous), then you are also able to fill in alternative names:

First Name (1), Middle Name (1), Last Name (1) and
First Name (2), Middle Name (2), Last Name (2).

LyncUri: If Skype for Business Integration is activated (see 8.1.12 Miscellaneous) then you will see this field and you can set the LyncUri (Skype for Business URI). On creation of a new user, this field will be default set to 'sip:' + email when you enter the email first.

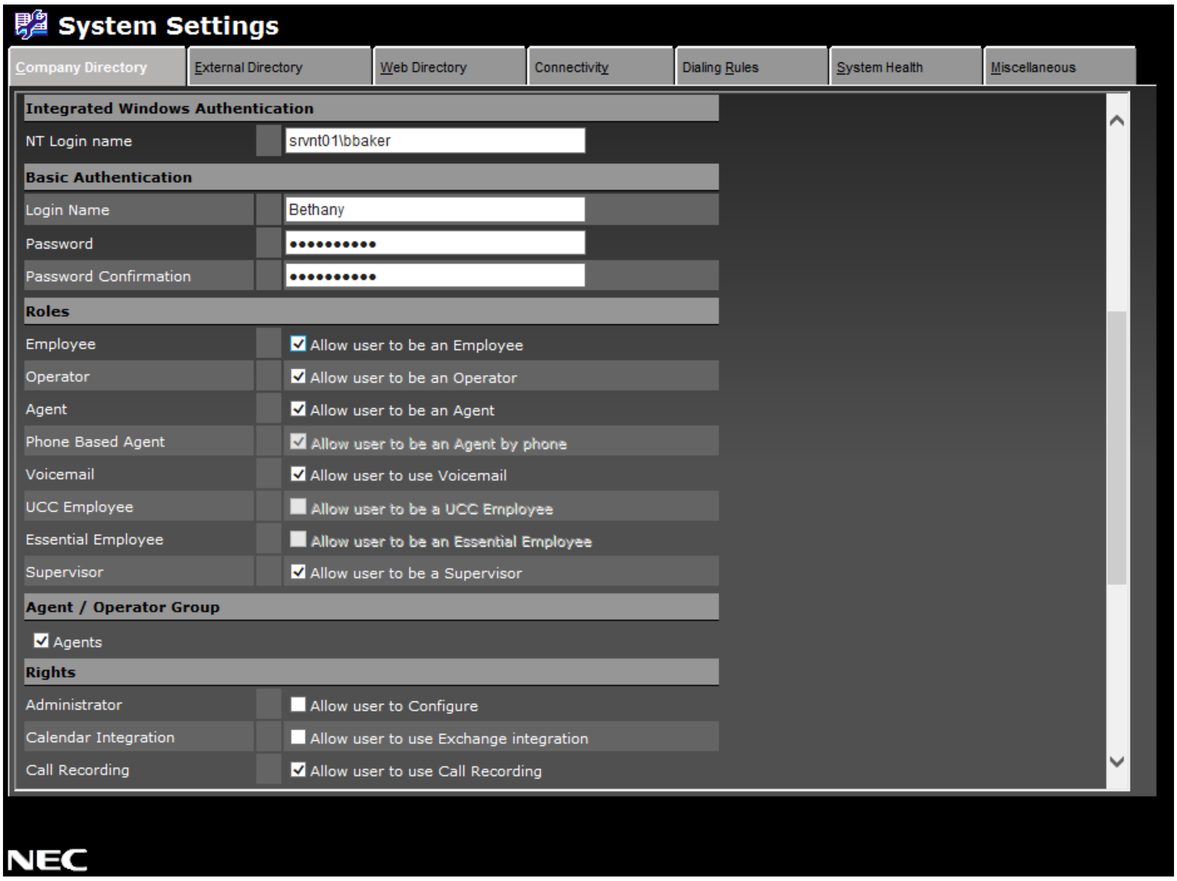
Profile Privacy: When checked, the contact details of this user will not be visible to any user (except for users who have administrator rights and for Agents/Operators of the same agent group).

Company Privacy Override: If Company Privacy is activated (see 8.1.12 Miscellaneous), then users cannot see contact data of other users belonging to other companies. If you want to override that for specific users (for instance operators working for all involved companies), then you need to activate this field.

5. Select the extension number and PBX of the new user from the drop down lists.

   Note: *If The selected extension is a special number (ACD group, start lines, routing points etc) and that number or any other number from the special number virtual group is already assigned for the special purpose, then the fields described in the steps 6 – 9 (NT Login name, Basic authentication section, Roles section, Agent/Operator group section, Rights section, Presence section, Voice mail and agent settings section) will not be visible.*

6. Enter Login Credentials for the BCT user. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.



Integrated Windows Authentication

NT Login name	srvnt01\bbaker

Basic Authentication

Login Name	Bethany
Password	••••••••••
Password Confirmation	••••••••••

Roles

Employee	☑ Allow user to be an Employee
Operator	☑ Allow user to be an Operator
Agent	☑ Allow user to be an Agent
Phone Based Agent	☑ Allow user to be an Agent by phone
Voicemail	☑ Allow user to use Voicemail
UCC Employee	□ Allow user to be a UCC Employee
Essential Employee	□ Allow user to be an Essential Employee
Supervisor	☑ Allow user to be a Supervisor

Agent / Operator Group

☑ Agents

Rights

Administrator	□ Allow user to Configure
Calendar Integration	□ Allow user to use Exchange integration
Call Recording	☑ Allow user to use Call Recording

Figure 8-58 Company Directory - Edit User part 2

7. Distribute the user roles by a mark in the appropriate tick-box.

- Select “Allow user to be an Employee” for BCT employees. “Voicemail” is checked by default, but can be unchecked to remove the voicemail functionality.

- Select “Allow user to be an Operator” if the user has the right to be an Operator.

- Select “Allow user to be an Agent” if the user has the right to be an Agent. “Phone Based Agent” will also be checked by default and cannot be manually unchecked.

- Select “Allow user to be an Agent by Phone” if the user has the right to be an “Agent by phone”.

- Select “Allow user to use Voicemail” if the user has voicemail access. This role may either be the only one checked (if the user only has voicemail access), or it may be combined with one or more of the following: “Employee”, ”Operator”, “Agent”, “Phone Based Agent.

- Select “Allow user to be an Essential Employee” if the user has the right to be an Essential Employee.

- Select “Allow user to use Skype for Business Integration” if the user has the right to be an UC Connector user.

- Select “Allow user to be OWI only” to grant the user the right to be an OWI user.
  This can only be selected when the user has no PBX selected.

- Select “Allow user to be a virtual agent for web chat on UIP client” if UIP integration is present in the system and user is meant to be a virtual agent (chat bot) powered by UIP.
  See Appendix W – Web Chat UIP Integration). This can only be selected when the user has no PBX selected.

- Select "Allow user to be a Supervisor" if the user needs the rights to use BCT Supervisor Dashboard client and BCT Supervisor Dashboard Client.

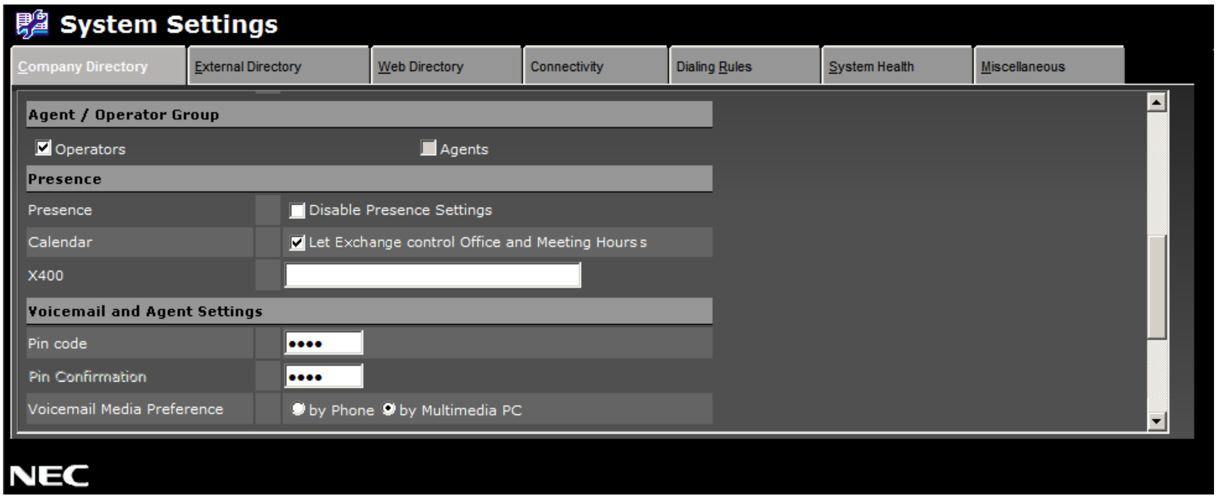
- Select “Allow user to Configure” if the user needs the right to do user administration.

- Select “Allow user to use Exchange integration” if the user wants to synchronize his/her presence settings with the Outlook Calendar by using Exchange Server integration. Per default the Exchange integration feature will also control Office and Meeting hours. This feature can be disabled in the presence part of the form (see below).

- Select “Allow user to use Call Recording” if the BCT user needs the right to record calls.

  Note: *Not all the roles can be assigned at the same time. Selecting particular roles will exclude the possibility to select other roles. Some roles cannot be selected if no extension was selected before.*

8. Select the default groups the user is a member of. Normally this is related to the Agent or Operator role of the user (or both). The groups can be shown in the Group and List pane.



Agent / Operator Group

☑ Operators ☐ Agents

Presence

Presence ☐ Disable Presence Settings

Calendar ☑ Let Exchange control Office and Meeting Hours s

X400

Voicemail and Agent Settings

Pin code ••••

Pin Confirmation ••••

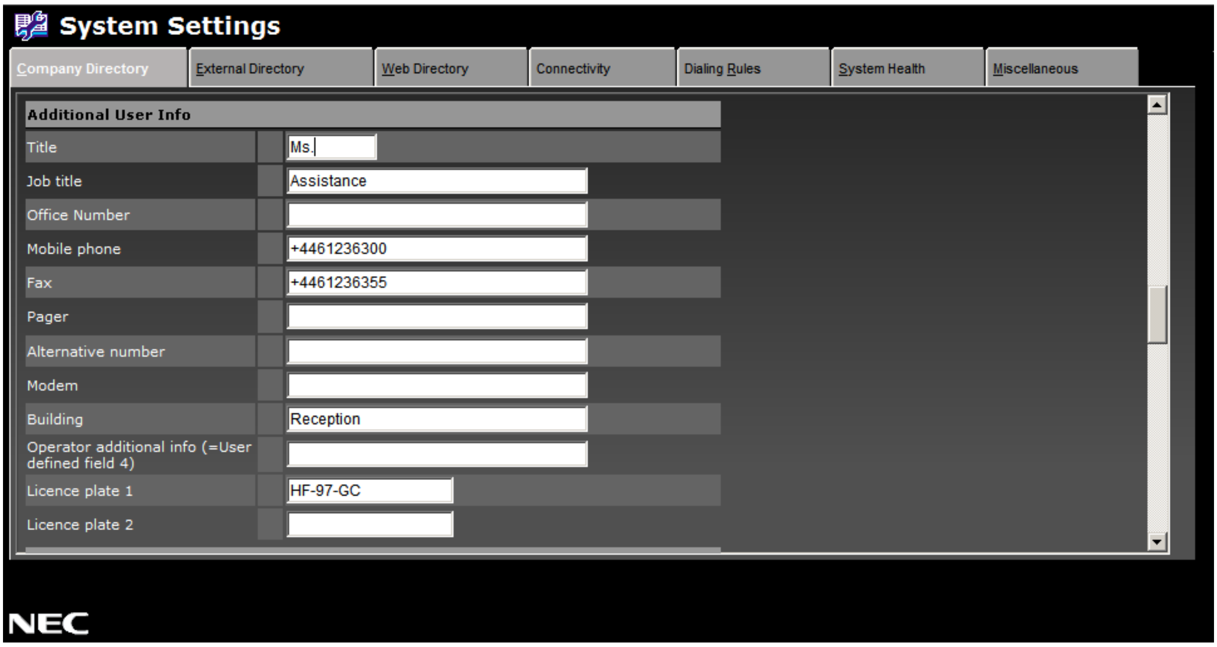
Voicemail Media Preference ○ by Phone ● by Multimedia PC

Figure 8-59 Company Directory - Edit User part 3

Select the required presence options. Per default presence is turned on for all users.

9. Enter the Pin code to be used for voicemail and / or Agent by Phone login. Without the Pin code the user cannot access voicemail from any telephone other than his/her own phone.

10. Enter Additional User info.

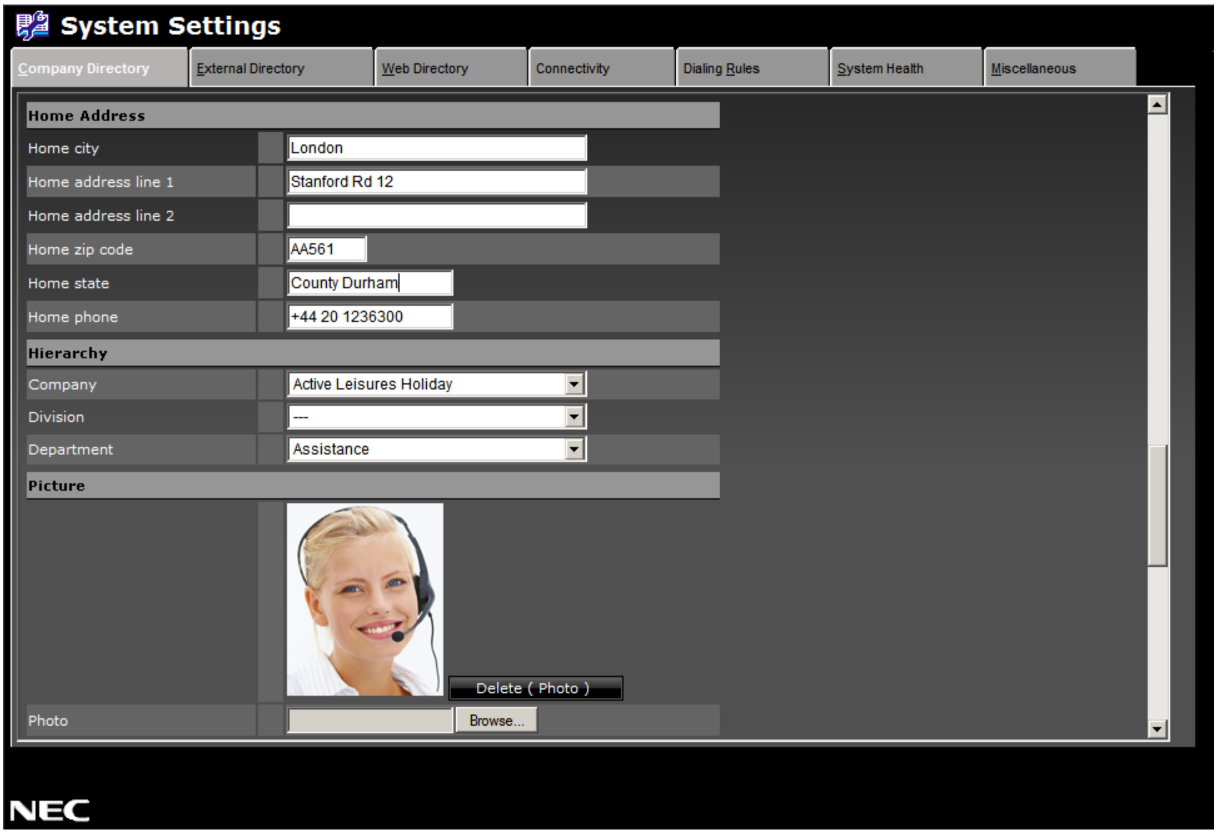


Additional User Info

Title	Ms.
Job title	Assistance
Office Number	
Mobile phone	+4461236300
Fax	+4461236355
Pager	
Alternative number	
Modem	
Building	Reception
Operator additional info (=User defined field 4)	
Licence plate 1	HF-97-GC
Licence plate 2	

Figure 8-60 Company Directory - Edit User part 4

11. Fill in Home Address fields



Home Address

Home city	London
Home address line 1	Stanford Rd 12
Home address line 2	
Home zip code	AA561
Home state	County Durham
Home phone	+44 20 1236300

Hierarchy

Company	Active Leisures Holiday
Division	---
Department	Assistance

Picture

Photo

Figure 8-61 Company Directory - Edit User part 5

12. Select the Company, Division and Department of the user from the appropriate lists. Add picture (if available)

13. In case you activated **Advanced editing** (see Figure 8-57 Company Directory - Edit User part 1), you will see a number of Custom String-Fields (1 up to 20). Each string-field is labelled as "Custom n" (translated in the local language).

    It is possible to enter alternative names for any of the "Custom n" string-fields, and thus also overrule any translation. To do that:

    - Open the Configuration Manager and select the configuration file ‘C:\Inetpub\wwwroot\Directory Browser\web.config’.
    - Locate the key : DB_TXT_eEV_PBC_empluser_1 (this is the "Custom 1" field)
    - Fill the value with the desired name, for example "Subgroup"
    - Press button Save to store the value.

In the System Setting page those "Custom n" string-field names will be replaced by the names you have assigned. You can use these string-fields also in the Full Directory and include them in any possible search / result option.

***Note:** These fields of the company directory can also be imported / exported.*

14. Press **Apply** to save the entry.

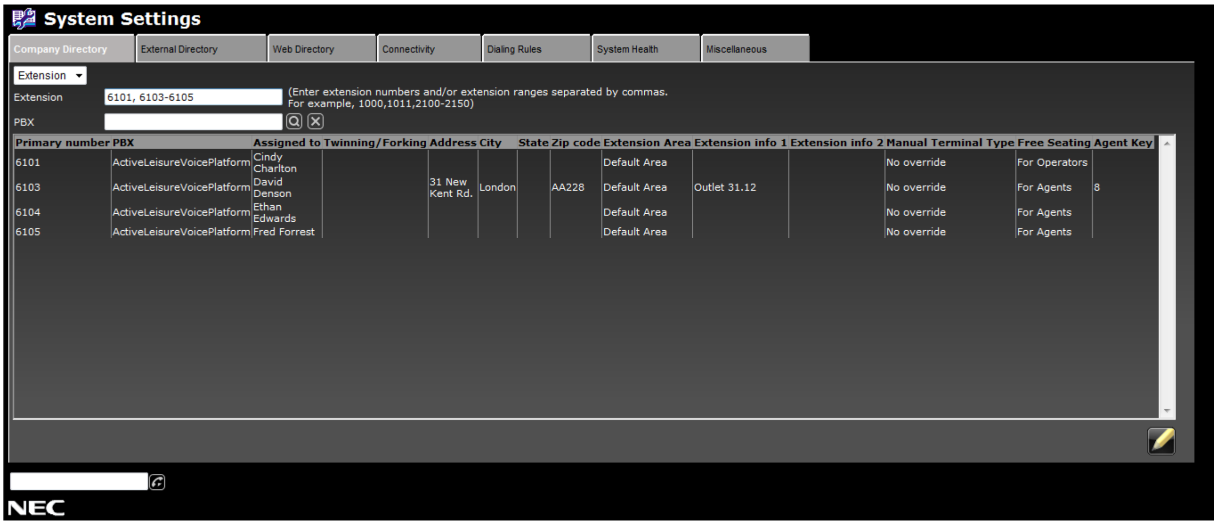
8.5.11. Edit or create a series and/or range of extensions

You can edit multiple extensions in one-go.

1. Login to BCT System Settings as ‘Administrator’.

2. Select **Extension** from the element selection box.

3. Enter your selection in the Extension field.
   Enter extension numbers and/or extension ranges separated by commas. For example: “2010-2020, 2400”.



System Settings

Extension: 6101, 6103-6105 (Enter extension numbers and/or extension ranges separated by commas. For example, 1000,1011,2100-2150)

PBX:

Primary number	PBX	Assigned to	Twinning/Forking	Address	City	State	Zip code	Extension Area	Extension info 1	Extension info 2	Manual Terminal Type	Free Seating	Agent Key
6101	ActiveLeisureVoicePlatform	Cindy Charlton						Default Area			No override	For Operators	
6103	ActiveLeisureVoicePlatform	David Denson		31 New Kent Rd.	London		AA228	Default Area	Outlet 31.12		No override	For Agents	8
6104	ActiveLeisureVoicePlatform	Ethan Edwards						Default Area			No override	For Agents	
6105	ActiveLeisureVoicePlatform	Fred Forrest						Default Area			No override	For Agents	

Figure 8-62 Multi editing

4. Press the **Edit** button (✎).

5. An Edit page will appear, filled with the common values. Make the required changes.

6. Press **Apply** to save the changes.

8.5.12. Changing a user's phone number

If an existing BCT user gets a new extension number in the PBX, you can either:

1. Delete the user from BCT and create the user again with the new extension number.

2. Remove all roles from the user, press Apply, answer the question about deletion of some user information. Change the extension number, press Apply. Re-assign the roles to the user.

3. Export all users in a csv-file, edit this file changing the extension number and import the modified file again.

Note: On change of the extension number the call-log will be deleted.

8.5.13. Website pop-up on incoming call

BCT clients can be configured in such a way that an external web-page pops up when a call is received. This is especially convenient for Contact Center Agents, because they can directly start searching in their own information system. Please read "BCT – Desktop Integrations" White Paper for more information.

8.5.14. Name ordering in directories

It is possible to select how a full name is composed. Names can be displayed as:

- First name, Middle name, last name or
- Last name "," First name, Middle name

This can be set via BCT System Settings / Miscellaneous / Fullname Composition.
Note that Fullname Composition also applies to alternative names (if you switched on "Search on alternative names").

8.5.15. Number to name translation

BCT uses translations of numbers to names. The name information is taken from the directories. This occurs for instance when detailed information of a call is displayed in the talk-zone of the BCT Desktop Client, or when Call Log or Voicemail Log entries are shown. Also the XML Client has number to name translations.

BCT will first try to find an exact match. If an exact match is not found, then it will try to find a match by removing most significant digits of the number (one by one), until it reaches the shortest allowed number length for number-recognition. Per default this shortest length is 7 digits. To change this default shortest length, follow the following steps:

1. Open the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config".

2. Locate the key: MatchShortestNumberSubstringLength

3. The default value is 7. Values 0 and 7 until 10 are allowed. In case of any other value, the default will be used.
   In case you specify the value "0" then BCT will only search for an exact match.

4. Press button Save to store the value.

5. Restart the Business ConneCT computer.

BCT will use standard Standard Telephone Number format (E164) for number to name translation. However, in Japan exact match in combination with the external directory will not work. To solve this, follow the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config”.

2. Locate the key: NameNumberMatchStrategy

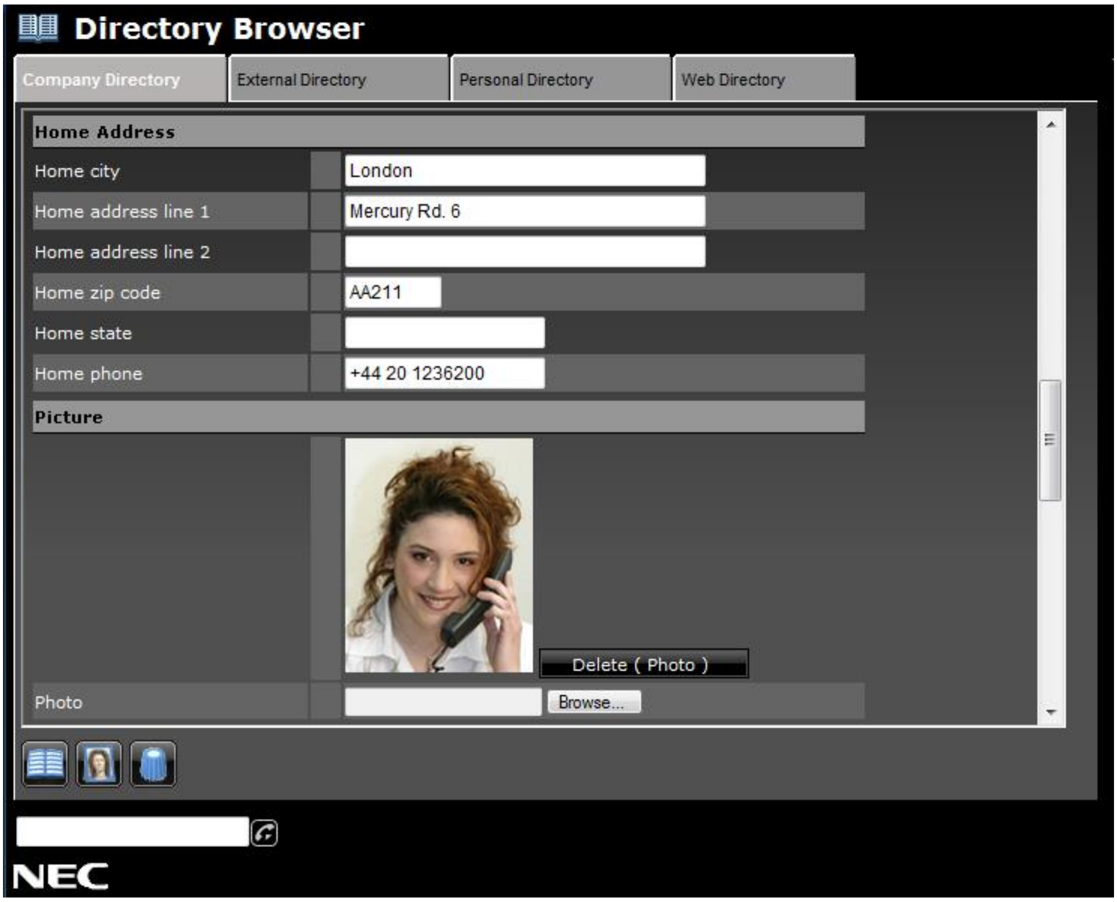
3. Change the entry to the desired value, for Japan it is "1". Values 0 and 1 are allowed. In case you specify "0", BCT will use E164 for an exact match.

4. Press button Save to store the value.

5. Restart the Business ConneCT computer.

8.5.16. Add a personal photo for a user

It is possible for the users to add a photo to their personal directory entry. This can be done “Set personal details” in the General tab of the BCT client settings.



Home Address	
Home city	London
Home address line 1	Mercury Rd. 6
Home address line 2	
Home zip code	AA211
Home state	
Home phone	+44 20 1236200
Picture	
Photo	

Figure 8-63 Personal details - add a photo

The photo is shown in the talkzone of the BCT client, on the DT700 / DT800 (BCT DT XML), on the BCT Mobile Client and in the Directory Browser.

The requirements for the photo are:

- Resolution: 100 x 133 pixels.
- Fileformat: jpg/jpeg.
- Filesize: about 5kb.

8.5.17. Copy number information from Full Directory to the Desktop Client

The integrated directory in the Desktop Client may not have enough fields and search criteria to find the right entry in the Company directory and External directory.

You can use the Full Directory to find the right entry. It will display the available numbers to dial.

By default you can click on any number to dial it. However, you can also configure it to copy the number you click on to the talkzone in the Desktop Client. It will also enable the buttons to select the required call functionality (dial, transfer, etc.).

To configure this:

1. Open the Configuration Manager and select the configuration file ‘C:\Inetpub\wwwroot\Directory Browser\web.config’.

2. Locate the following keys: PreDialForEmployee, PreDialForAgent and PreDialForOperator

3. For each of these roles "True" enables copying the number, "False" enables dialing the number.

4. Press button Save to store the values.

8.6. Configuring redundant PBX configurations

The following redundant PBX configurations can be configured:

- SV8500/SV9500 Location Diversity.
- Redundant 3C configuration.
- SIP@Net Dual Server WAN and Server Cluster WAN.
- SV9500 Geographic Redundancy.

Note: *In SIP@Net redundant LAN configurations the redundancy is handled completely within the boundaries of the PBX, no additional actions for failover of BCT are required.*

Note: *Selection between SV8500/SV9500 Location diversity or SV9500 Geographic redundancy is made during synchronization of BCT: depending on ASYDL settings (see paragraph* 4.3.13 SV9500 configuration for Geographic Redundancy*) an SV9500 system is detected as location diversity or Geo redundant system.*

Nodes of a redundant PBX network are defined as follows:

- *Master node*: the node of the network that controls the network.
  It is the node where BCT will connect to.

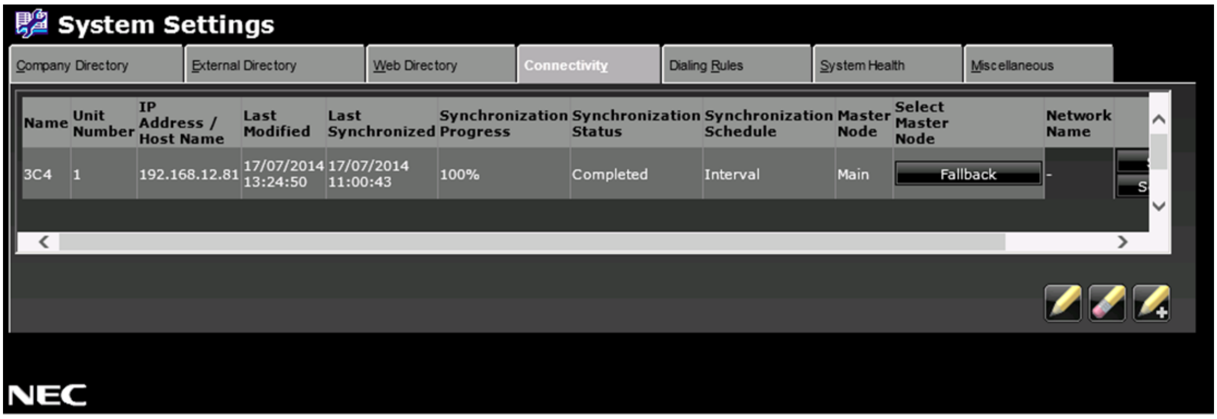
- *Main node*: the node that is the default Master node of the network.

- *Fallback node*: the node that is used as Master node when for some reason the Main node is not available.
  This can be due to failure of the Main node, or for maintenance reasons.
  Dependent of the type of PBX, 'Main' and 'Fallback' can have slightly different meanings.
  In a 3C system and in SIP@Net Dual Server WAN, the Main and Fallback are equivalent with respect to PBX functionality, while in an SV8500/SV9500 (or SV9500-Geo) and in SIP@Net Server Cluster WAN the PBX distinguishes between Main and Fallback.

Using redundant PBX configurations requires the license "Location diversity". The connection between BCT and the PBX is configured in the "Connectivity tab" of the BCT System Settings (see Figure 8-64 The System Settings Connectivity tab).

Settings specific for a PBX can be configured in the PBX Info tab, opened by either double-click the PBX in the connectivity tab, or by selecting the PBX and pressing the 'Edit' button at the bottom of the page. In the PBX Info tab, redundancy can be configured for a PBX.

When redundancy is configured for a PBX that supports manual failover, the connectivity tab contains two extra buttons, "Main" and "Fallback". These buttons can be used to switch manually between the Master and the Fallback PBX. See Figure 8-64 The System Settings Connectivity tab.



Name	Unit Number	IP Address / Host Name	Last Modified	Last Synchronized	Synchronization Progress	Synchronization Status	Synchronization Schedule	Master Node	Select Master Node	Network Name
3C4	1	192.168.12.81	17/07/2014 13:24:50	17/07/2014 11:00:43	100%	Completed	Interval	Main	Fallback	-

Figure 8-64 The System Settings Connectivity tab

When the PBX must support redundancy this must be configured in the PBX Info tab. When the radio button ‘Yes’ is selected for the ‘Support Failover’ or ‘Support Location Diversity’ setting, additional items become visible:

- **Failover Mode (not for SIP@Net or SV9500-Geo)**:
  The following options can be selected:
  - **Manual**: automatic failover is disabled. Manual failover can be done via the buttons on the Connectivity tab (see Figure 8-64 The System Settings Connectivity tab).
  - Automatic: automatic failover is done to the other node when the current active node fails. Manual failover can always be done.

    By default the delay before an automatic failover is done is 6 minutes. Delay times can be adapted in the configuration file of Redundancy Service:
    - *Open the Configuration Manager and select the configuration file "C:\Program Files (x68)\Common Files\NEC\Services\RedundancyService.WinService.exe.config".*
    - Search for key RedundancyService.DelayBeforeFailoverInMinutes
    - The delay between the detection of a non functional connection and the fail over to the other node. Default: 6 minutes
    - Locate key RedundancyService.FailoverRetryPeriodInMinutes
    - The period between retries when failing over fails. Default: 6 minutes
    - Locate key RedundancyService.DelayBeforeFailbackInSeconds
    - The delay between switch back from fallback to the main. Default: 0 seconds
    - Press button Save to store the values
    - Restart the Redundacy service.

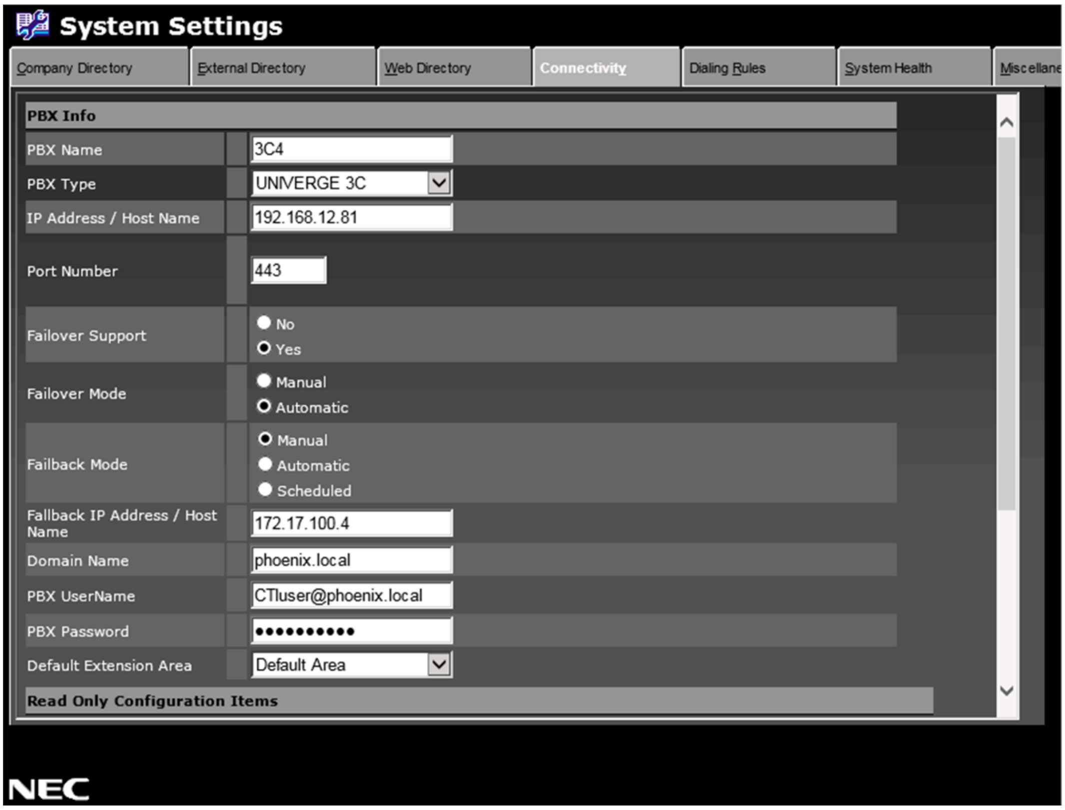
- **Failback Mode (not for SIP@Net or SV9500-Geo)**:
  - **Manual**: automatic failback is disabled. Manual failback can be done via the buttons on the Configuration tab (see Figure 8-64 The System Settings Connectivity tab).
  - **Automatic**: automatic failback is done when the fallback node is active and the preferred node becomes available again.
    After a manual failover no automatic failback will be done, a manual failback is the usual way to switch back to the preferred node.
  - **Scheduled**: a schedule time can be configured when the system must failback to the preferred node when the fallback node is active (see Figure 8-66 Configuration of 3C redundant system: scheduled fallback). Manual failback can always be done.

NB: When Failover Mode 'Manual' is selected, only 'Manual' is allowed for the failback action (see Figure 8-65 Configuration of 3C redundant system: manual failover). All failover and failback actions are under manual control.

- **Failover Configuration (SIP@Net only):**
  Select the redundant configuration as projected in the SIP@Net Pbx. Possible options:
  - **SIP@Net Dual Server WAN.**
  - **SIP@Net Server Cluster.**
- **Preferred Server (SIP@Net Server Cluster only):**
  - **Main Server:** when both SIP@Net servers are reachable, e.g. due to a WAN failure, BCT will failover to the main node. Select this option when the most (important) BCT clients are located on the WAN segment of the main node (see Figure 8-67 Configuration of SIP@Net Server Cluster).
  - **Fallback Server:** when both SIP@Net servers are reachable, e.g. due to a WAN failure, BCT will failover to the fallback node. Select this option when the most (important) BCT clients are located on the WAN segment of the fallback node.
- **Fallback IP Address/Hostname**:
  The hostname or IP address of the secondary server that will be used as Fallback node.
  For SV8500/SV9500 the address of the Fallback node can be selected from a dropdown list, for SV9500-Geo, 3C or SIP@Net system the address must be entered manually.

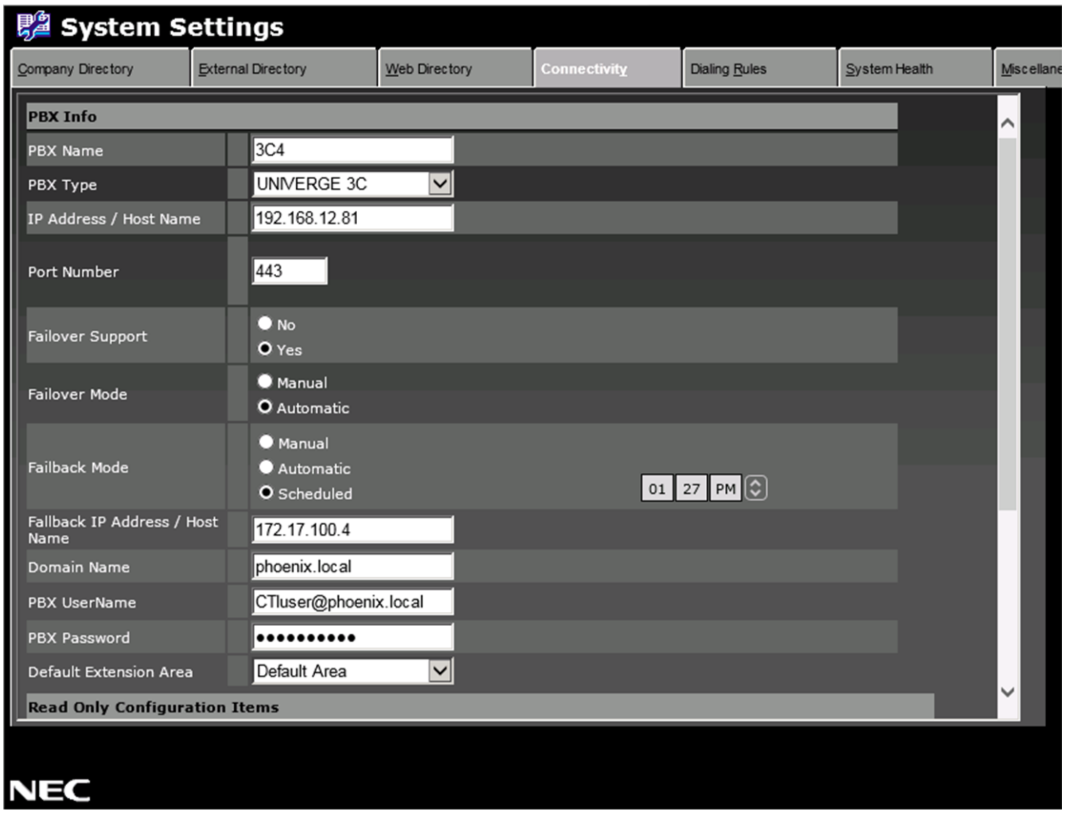
Note: *When a new SV8500/SV9500 (or SV9500-Geo) system is created in BCT, it must be synchronized first before location diversity/Geographic redudancy can be defined.*

Note: *In case of redundant SIP@Net or SV9500-Geo the PBX determines which node is active, manual or scheduled failover/failback from BCT is not supported. When Failover Support is defined for a SIP@Net or SV9500-Geo PBX this is always automatic failover.*



PBX Info	
PBX Name	3C4
PBX Type	UNIVERGE 3C
IP Address / Host Name	192.168.12.81
Port Number	443
Failover Support	○ No ● Yes
Failover Mode	○ Manual ● Automatic
Failback Mode	● Manual ○ Automatic ○ Scheduled
Fallback IP Address / Host Name	172.17.100.4
Domain Name	phoenix.local
PBX UserName	CTIuser@phoenix.local
PBX Password	••••••••••
Default Extension Area	Default Area
Read Only Configuration Items	

Figure 8-65 Configuration of 3C redundant system: manual failover

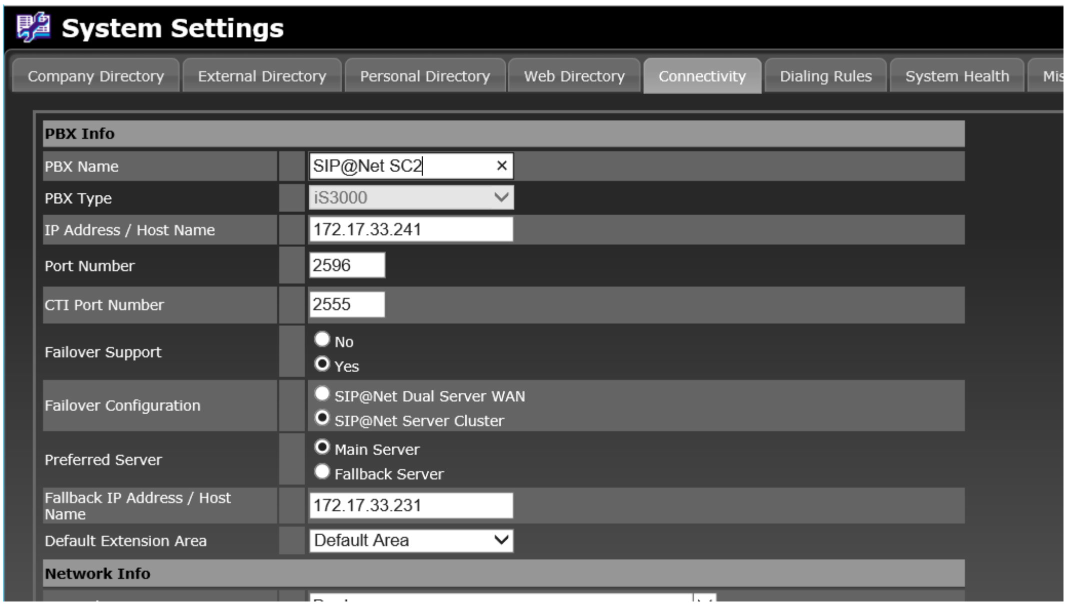


PBX Info

PBX Name	3C4
PBX Type	UNIVERGE 3C
IP Address / Host Name	192.168.12.81
Port Number	443
Failover Support	○ No ● Yes
Failover Mode	○ Manual ● Automatic
Failback Mode	○ Manual ○ Automatic ● Scheduled 01 27 PM
Fallback IP Address / Host Name	172.17.100.4
Domain Name	phoenix.local
PBX UserName	CTIuser@phoenix.local
PBX Password	••••••••••
Default Extension Area	Default Area

Read Only Configuration Items

Figure 8-66 Configuration of 3C redundant system: scheduled fallback



PBX Info

PBX Name	SIP@Net SC2
PBX Type	iS3000
IP Address / Host Name	172.17.33.241
Port Number	2596
CTI Port Number	2555
Failover Support	○ No ● Yes
Failover Configuration	○ SIP@Net Dual Server WAN ● SIP@Net Server Cluster
Preferred Server	● Main Server ○ Fallback Server
Fallback IP Address / Host Name	172.17.33.231
Default Extension Area	Default Area

Network Info

Figure 8-67 Configuration of SIP@Net Server Cluster

General Notes for SV8500/SV9500 Location Diversity (not for SV9500-Geo):

1. DDI fail for Operator requires a real terminal (so virtual number is not working). This terminal must also have Location Diversity.

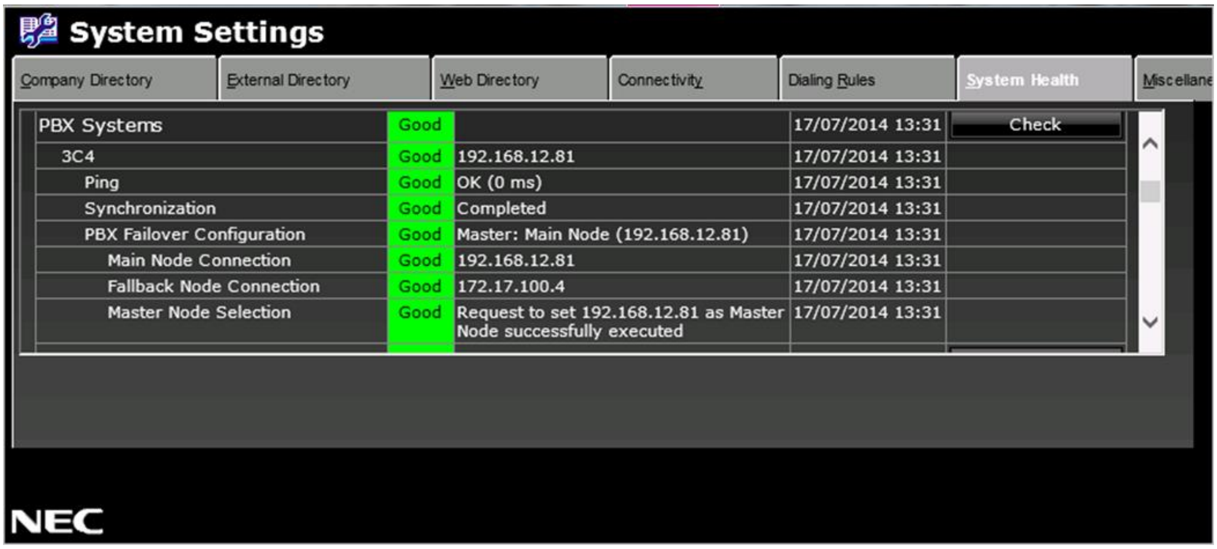
2. For Agent functionality (SV8500/SV9500 only), all contact center access numbers must be assigned as sub-line to a terminal which has Location Diversity.

3. To support fallback routing in the PBX, make all contact center access numbers a routing point in BCT.

4. Synchronize the time of "PBX force the extensions to recover" as specified in the BCT connection tab. If it is every day on a specific time, set the recovery-time in the PBX 10 minutes earlier.
   If there is no daily recovery, set the recovery time in the PBX on never.

The PBX Systems component of the System Health contains the redundant PBX system. It contains a number of settings for the redundant configuration. The Services component of the System Health contains the “Redundancy Service” and it will show status of the service. See Figure Figure 8-68 Health Check with redundant configuration.

Note: *When changes are made regarding IP-addresses of the nodes a Synchronization is required for SV8500/SV9500 and SV9500-Geo.*



PBX Systems	Good		17/07/2014 13:31
3C4	Good	192.168.12.81	17/07/2014 13:31
Ping	Good	OK (0 ms)	17/07/2014 13:31
Synchronization	Good	Completed	17/07/2014 13:31
PBX Failover Configuration	Good	Master: Main Node (192.168.12.81)	17/07/2014 13:31
Main Node Connection	Good	192.168.12.81	17/07/2014 13:31
Fallback Node Connection	Good	172.17.100.4	17/07/2014 13:31
Master Node Selection	Good	Request to set 192.168.12.81 as Master Node successfully executed	17/07/2014 13:31

Figure 8-68 Health Check with redundant configuration

9. CLIENT INSTALLATION AND CONFIGURATION

Below a summary can be found of the available BCT related client applications (packages):

- Desktop Client – PC
- Client Integration - PC
- Contact Center (Supervisor) Client – PC
- Soft Wallboard – PC
- Mobile Client – Smart Phone
- BCT Agent – Smart Phone
- XML Client – DT Terminal
- UC Connector – PC
- Salesforce Open CTI Adapter – PC

9.1. Desktop Client - PC

Note: *We strongly recommend both client PC and server PC join the same Windows domain.*

The BCT Desktop Client is an application that runs on a PC and is used by end users having the employee, agent and/or operator role.

9.1.1. Desktop Client Installation

The BCT Desktop Client requires the next prerequisite to be installed on the client PC (see also 2.3 Client PC requirements):

- Microsoft .NET Framework 4.8
  This specific version is not by default available on all supported Windows versions, so deployment might be needed.

The BCT Desktop client is typically designed to be deployed using the Microsoft-defined ClickOnce deployment technology. One benefit of ClickOnce is the support for automatic updates. Deployment of the BCT Desktop Client using ClickOnce is offered in 2 flavors:

1. Installation via Installation Portal (web page), i.e. pull installation.
2. Installation via (bootstrap) MSI package (for pushed installations)

Note: *The ClickOnce deployment approach does not fully function in a Citrix or Terminal Services environment. The main cause is that for ClickOnce the application files are downloaded into a local cache folder, which is located in the non-roaming user profile section.*

For this reason, as an alternative, a straight-forward MSI based installation package is offered. You can install it as described in 9.1.1.2 Installation via (bootstrap) MSI package (for pushed installations) or use the DVD autorun menu item "Desktop Client (Special)".

Once more, be aware of the accompanied remark: “Only use this in a Citrix or Terminal Services context”. Clients deployed using this menu entry will lack automatic upgrade support".

9.1.1.1. Installation via Client Portal (web page)

***Note**: Installation of the 'Desktop Client' using ClickOnce deployment via the 'Client Portal' web site is natively only supported using "Internet Explorer" or "Edge" browser.*

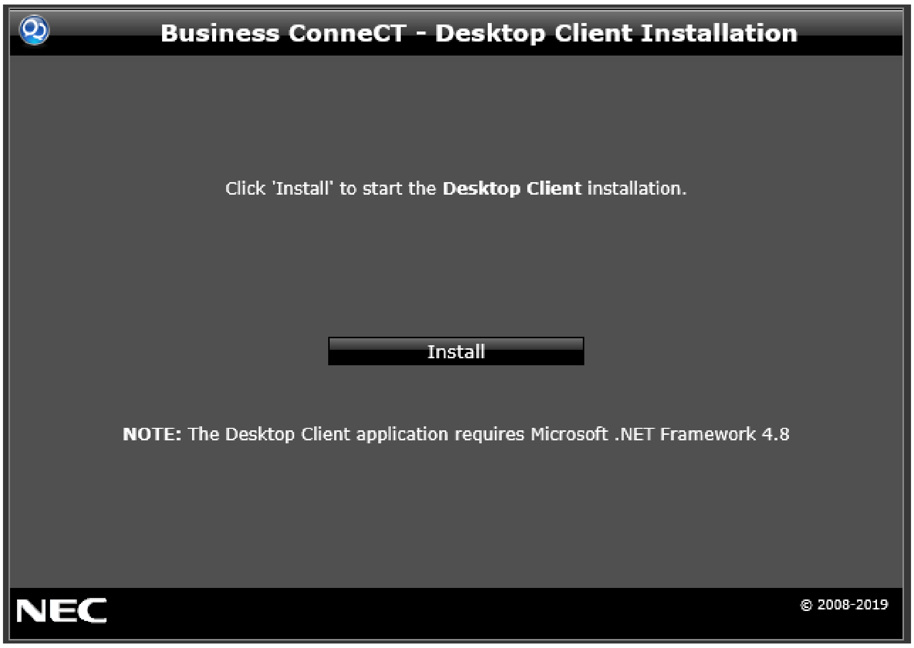
For 'Edge Chromium' browser it is required to explicitly enable 'ClickOnce Support' using:

- *Edge feature flag 'edge://flags/#edge-click-once'*
- *Edge group policy 'Allow users to open files using the ClickOnce protocol'*

To install (and directly start) the BCT Desktop Client on first use, the user must use the following hyperlink:

```
http://<servername>/BCT/default.asp
```

The <servername> is the name of the BCT server. This will show the screen as shown below. The setup will start when you click the Install button.



Business ConneCT - Desktop Client Installation

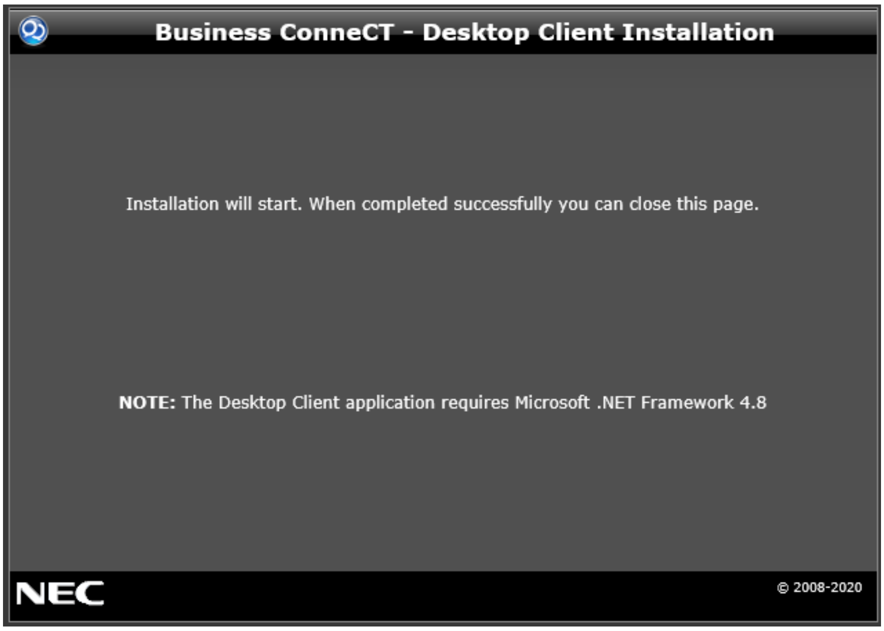
Click 'Install' to start the **Desktop Client** installation.

NOTE: The Desktop Client application requires Microsoft .NET Framework 4.8

***Note:** To install the required Microsoft .NET Framework 4.8 you can use the install option offered in the **BCT DVD Main Menu**.*

***Note:** To install the Microsoft .NET Framework 4.8 you need to have Administrator rights. If you lack these rights ask your system administrator to deploy it.*

When you have initiated the install the screen will show as below. So wait until the client application is started and close the browser page. For subsequent starts use the entry created in the start menu or configure the client to start automatically after windows logon.



Business ConneCT - Desktop Client Installation

Installation will start. When completed successfully you can close this page.

NOTE: The Desktop Client application requires Microsoft .NET Framework 4.8

9.1.1.2. Installation via (bootstrap) MSI package (for pushed installations)

There is also a single MSI package available for deployment of the desktop client. This MSI file “Business ConneCT Client.msi” is located on the DVD in folder “D:\Business ConneCT 12.00\DesktopClient\MSI\ClickOnce\DISK1” (assuming D: is DVD drive letter).

To deploy clients using this MSI file please use next command:

```
msiexec.exe /i "Business ConneCT Client.msi" /qn SERVERNAME=<BCTSERVER>
```

where <BCTSERVER> is the hostname of the BCT server.

Note: *To use MSI deployment in a Citrix environment: Use the MSI file ‘DesktopClient.Standard.msi’ located in folder "D:\Business ConneCT 12.00\DesktopClient\MSI\Special\DISK1” (assuming D: is DVD drive letter). Deploy with:*

```
msiexec.exe /i "DesktopClient.Standard.msi" /qn SERVERNAME=<BCTSERVER>
```

Note: *To uninstall the client MSI deployed package run:*

```
msiexec /x "{9F9EEB6C-E358-4A35-BCAE-029314862CCA}" /qb
```

or in case of Citrix related client MSI:

```
msiexec /x "{B4D00E78-504A-4153-85C1-A83A726FCBE6}" /qb
```

9.1.2. Desktop Client Configuration

Local defined BCT Desktop Client applications settings (like control of client logon / logoff) can be configured via ‘Settings’ button. For details please refer to the BCT User Guide.

Also global configuration settings can be defined via the BCT server. Below a list of configurable server side settings related to the BCT Desktop Client.

9.1.2.1. Outlook Contact Popup settings

The Desktop Client can display an Outlook contact card of caller with an incoming call.
For settings see Appendix F – OUTLOOK CONTACT POPUP SETTINGS

9.1.2.2. Desktop Client – Operator Configuration

See chapter 8.3 - Operator configuration

9.1.2.3. Configure voicemail to email integration

More information about the configuration can be found in section 8.1.10.1 Configure Voicemail to Email (Unified Messaging).

9.1.2.4. Configure Microsoft Outlook (calendar) integration

On the server via “System Settings > Company Directory > Edit User” select under ‘Rights’ option “Allow user to use Exchange Integration” for each BCT user. The customer needs the license "Employee-Outlook Calendar Integration" for this functionality.

Note: *The BCT user can also enable / disable Outlook calendar synchronization via “Settings”, “General tab” and use the box “Enable Exchange calendar synchronization” within the client application.*

Note: *Synchronization between the BCT scheduler and Microsoft Outlook calendar is controlled by BCT.*

Note: *For more information on how to configure integration for Microsoft Exchange: see 21 Appendix K – EXCHANGE INTEGRATION.*

9.2. Client Integration – PC

Besides the Desktop Client deployment package there is an additional “Client Integration” package that offers the next features:

1. Hotkey Dialer
   With Hotkey Dialer you can dial any selected number by pressing a function key (e.g. F8)

2. LLDP Single Sign On
   With Single Sign On, the default extension number of a user is moved to the telephone set when a user logs on in Windows, connects to the internet or docks his/her PC.
   Note: *This feature is only applicable (visible) when target operating system is Windows 7, Windows 8.1 or Windows 10.*

3. Call Handling TSP
   Call Handling TAPI Service Provider used to dial for example from contact in Microsoft Outlook (using dialer URL on Business ConneCT Server)

4. Supervisor Dashboard
   The Supervisor Dashboard is a day-to-day monitoring tool for your contact center and for the group of agents under your supervision.
   Notes:
   This feature is not applicable (visible) when target system has installed BCT Server or Contact Center Client.
   Requires “Microsoft System CLR Types for Microsoft SQL Server 2017” as prerequisite (see below).

This package requires the next prerequisite to be installed on the client PC (see also 2.3 Client PC requirements):

- Microsoft .NET Framework 4.8
  This specific version is not by default available on all supported Windows versions, so deployment might be needed.

- Microsoft Visual C++ 2017 Runtime (x86)
  This prerequisite can be installed from the **BCT DVD Main Menu** window (i.e. select ‘Microsoft Visual C++ 2017’ under ‘Supporting Application’ section.

- Microsoft System CLR Types for Microsoft SQL Server 2017 (required for Supervisor Dashboard)
  This prerequisite MSI package named “SQLSysClrTypes.msi” can be obtained (installed) from the **BCT DVD** folder “D:\Business ConneCT 12.00\ContactCenterClient\Prerequisites\Bin”

Note: *Starting from BCT 8.10.x the hotkey dialer functionality is integrated in the ‘Desktop Client’ application (so for hotkey dial functionality there is no need anymore to install optional ‘Client Integration’ package). The hotkey dialer functionality is still offered as feature in ‘Client Integration’ to have a hotkey dialer stand-alone solution. When both are installed the ‘Desktop Client’ application will take precendence for hotkey dialing when it is running.*

Note: *The BCT Desktop Client itself offers Microsoft Outlook integration to use the Outlook calendar for presence and to initiate an Outlook contact pop-up for incoming calls.*

9.2.1. Client Integration Installation

You can install the Client Integration software package on the client:

1. Via the option called "Client Integration" offered by the BCT autorun.exe application (started via auto play of DVD - if not automatically started do run D:\Autorun.exe - where D is DVD drive letter) or...

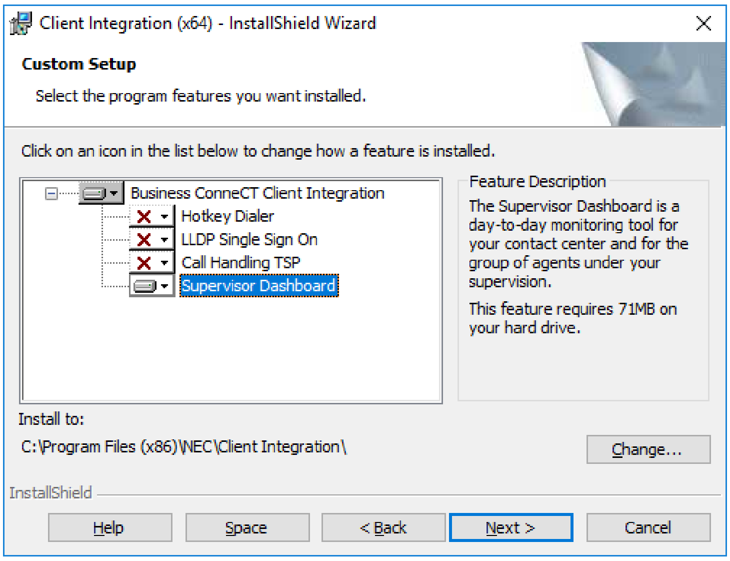
2. Using the single MSI package intended for pushed installations (e.g. via logon scripts). So rollout of the package in a corporate environment (e.g. using GPO or SCCM).

9.2.1.1. Client Integration Installation - Interactive

When the installation is initiated from Autorun.exe the "Client Integration" package will show a welcome dialog.

1. In the welcome screen select **Next**

1. In “Custom Setup” dialog now select the feature(s) you would like to install.



Client Integration (x64) - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Business ConneCT Client Integration
  - ☒ Hotkey Dialer
  - ☒ LLDP Single Sign On
  - ☒ Call Handling TSP
  - Supervisor Dashboard

Feature Description

The Supervisor Dashboard is a day-to-day monitoring tool for your contact center and for the group of agents under your supervision.

This feature requires 71MB on your hard drive.

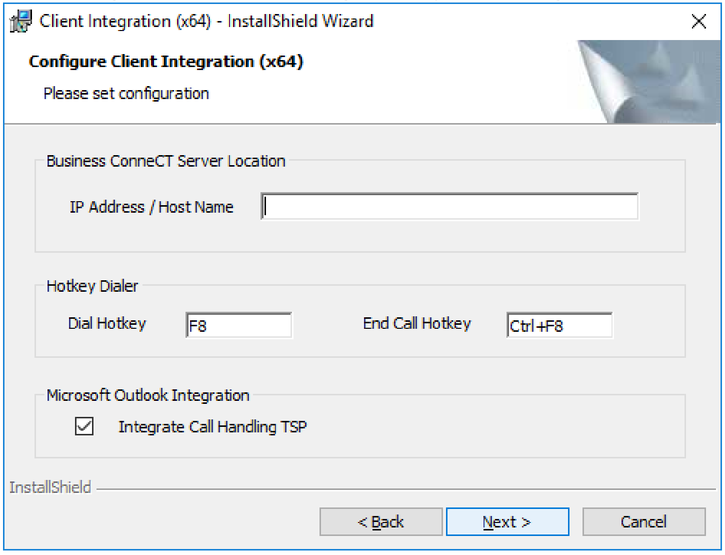
Install to:

C:\Program Files (x86)\NEC\Client Integration\

***Note:** By default all features are disabled so you are enforced to explicitly select one or more.*

2. Select Next

3. In “Configure Product” dialog enter your configuration settings.



Client Integration (x64) - InstallShield Wizard

Configure Client Integration (x64)

Please set configuration

Business ConneCT Server Location

IP Address / Host Name

Hotkey Dialer

Dial Hotkey: F8

End Call Hotkey: Ctrl+F8

Microsoft Outlook Integration

☑ Integrate Call Handling TSP

__Note:__ Hotkey Dialer configuration is only visible when ‘Hotkey Dialer’ feature is selected.

__Note:__ Microsoft Outlook Integration configuration is only visible when ‘Call Handling TSP’ feature is selected and when local installed Outlook is detected.

4. Select Next

5. Select Install to start the installation

6. After installing the software, configure as specified in the following sections.

9.2.1.2. Client Integration Installation – Silent

Besides the interactive installation using setup.exe the "Client Integration" package offers also a single MSI package for silent installation.

- For 32-bit Windows versions use MSI file "Client.Integration.x64.msi" from "D:\Business ConneCT Resources\Optional Packages\Client Integration\Client.Integration.x86\MSI\DISK1"

- For 64-bit Windows versions use MSI file "Client.Integration.x64.msi" from "D:\Business ConneCT Resources\Optional Packages\Client Integration\Client.Integration.x64\MSI\DISK1"

When using the MSI from the command line for installation or upgrade at least one feature must be defined (using ADDLOCAL). The possible feature names are:

- Hotkey.Dialer
- LLDP.SSO
- CallHandling.TSP
- Supervisor.Dashboard

When using the MSI from the command line, the feature selection as well as configuration settings can be defined using properties. See below an explanation of available properties:

ADDLOCAL	Comma delimited list that defines features to be installed. To install all features locally, use ADDLOCAL=ALL
REMOVE	Comma delimited list that defines features that are to be removed. To remove all features, use REMOVE=ALL
SERVERNAME	Defines the BCT server hostname or IP address.
OUTLOOKINTEGRATION	Defines whether to integrate Call Handling TSP with Outlook (0=No, 1=Yes).
DIALHOTKEY	Defines the default hotkey to initiate a call using Hotkey Dialer (e.g. F8).
CALLENDHOTKEY	Defines the default hotkey to end a call started via Hotkey Dialer (e.g. Ctrl+F8).

1. Initial and upgrade installation of Client Integration package:
   It is required to explicit define one or more features to be installed.

   Syntax examples for MSI:

```
msiexec /i Client.Integration.x64.msi ADDLOCAL=Hotkey.Dialer,
Supervisor.Dashboard SERVERNAME=<servername> DIALHOTKEY=F8 CALLENDHOTKEY=Ctrl+F8
/qb

msiexec /i Client.Integration.x64.msi ADDLOCAL=CallHandling.TSP
SERVERNAME=<servername> OUTLOOKINTEGRATION=1 /qb
```

```
msiexec /i Client.Integration.x64.msi ADDLOCAL=Supervisor.Dashboard
SERVERNAME=<servername> /qb

msiexec /i Client.Integration.x64.msi ADDLOCAL=Hotkey.Dialer
REMOVE=Supervisor.Dashboard SERVERNAME=<servername> DIALHOTKEY=F7
CALLENDHOTKEY=Ctrl+F7 /qb

msiexec /i Client.Integration.x64.msi ADDLOCAL=LLDP.SSO SERVERNAME=<servername>
/qb
```

2. Uninstall of the Client Integration package:

```
msiexec /x Client.Integration.x64.msi /qb
```

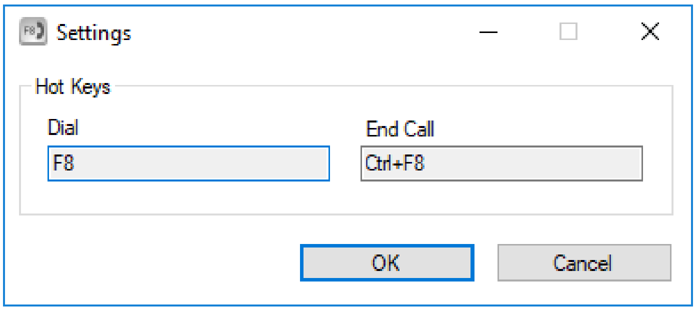
9.2.2. Client Integration Configuration

9.2.2.1. Hotkey Dialer Configuration

First of all you also have to configure BCT server to use *Integrated Windows Authentication*. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.

The hotkey dialer application is automatically started after installation and is visible as icon in the traybar. The default function keys for start (F8) and end a call (Ctrl+F8) are defined during installation time. However, one can change it afterwards by using the settings dialog (right mouse menu on traybar icon).

Dialog looks like below:



Settings

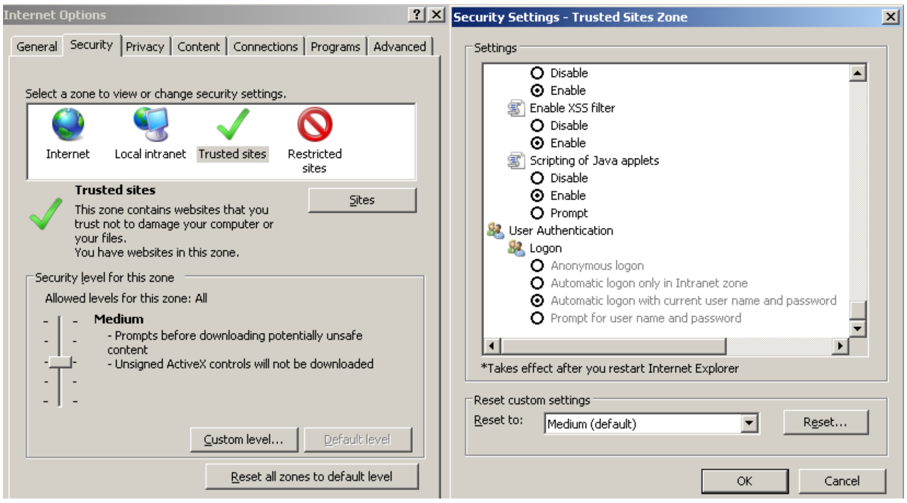
Hot Keys

Dial: F8

End Call: Ctrl+F8

Figure 9-1 Hotkey Dialer settings

Note: *If the Hotkey Dialer does not work, then this may be solved by changing User Authentication in your Internet Explorer settings to "Automatic login with current user name and password", as pictured in* Configuring Internet Explorer settings for Hotkey Dialer



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Sites

Security level for this zone

Allowed levels for this zone: All

Medium
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

Custom level... | Default level

Reset all zones to default level

Security Settings - Trusted Sites Zone

Settings

○ Disable
● Enable
Enable XSS filter
○ Disable
● Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
○ Automatic logon only in Intranet zone
● Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium (default) | Reset...

OK | Cancel

Figure 9-2 Configuring Internet Explorer settings for Hotkey Dialer

9.2.2.2. LLDP Single Sign On Configuration

With Single Sign On, the default extension number of a user is moved to the telephone set when a user logs on in Windows, connects to the internet or docks his/her PC. The extension number is removed from the telephone set when the user logs off, disconnects or undocks.

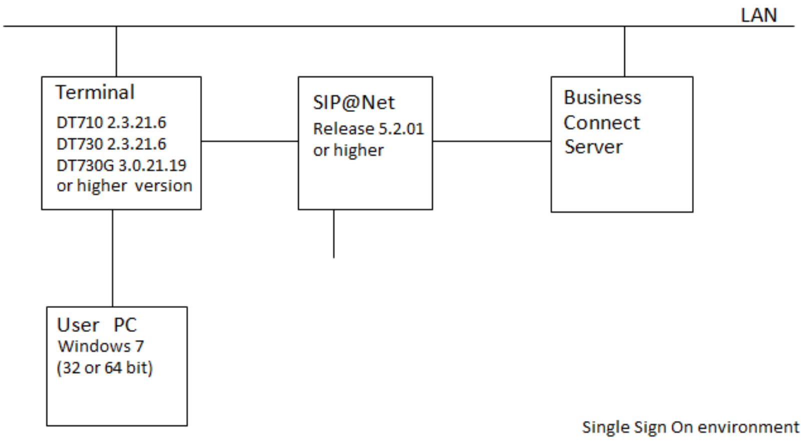


Figure 9-3 Single Sign On Environment

The requirements to the Single Sign On environment are shown in Figure 9-3 Single Sign On Environment. The User PC is connected to the LAN via the LAN port of the telephone terminal.

Note: *The LLDP Single Sign On package provides support of the LLDP protocol for automatic terminal recognition on the Network Interface Connections. The package contains a LLDP Protocol driver (LLDP NDIS Protocol Driver). The protocol driver is enabled by default for all Network Interface Cards. When you have more than one Network Interface Card in your PC, you can select the one to use.*

Note: *Since the LLDP Protocol driver is Windows platform specific a Windows upgrade from for example Windows 7 to Windows 10 will require the “Client Integration” to be uninstalled and reinstalled.*

SIP@Net Configuration

For a BCT user to access following functionality, it is required to assign the following facility class mark (FCM) to the user's extension:

- FCM 57 - Desk-sharing entitled

Terminal Configuration

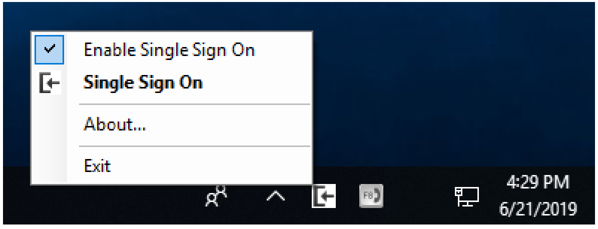
LLDP mode must be enabled:

1. Go to Menu – Admin settings.
2. Enter admin username and password.
3. Select 'Network Settings'.
4. Select 'Advanced Settings'.
5. Select 'LLDP Mode'.
6. Select 'Enable LLDP'.
7. Press OK and reboot the terminal.

Business ConneCT Configuration

First of all you also have to configure BCT server to use *Integrated Windows Authentication*. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.

The LLDP SSO Configurator application is automatically started after installation and is visible as icon in the traybar. Single Sign On has to be enabled before you can use it. This can be done via right mouse menu on traybar icon. See dialog below:



When enabled, the menu entry 'Single Sign On' can be selected to open the Single Sign On configuration screen. This screen looks like:

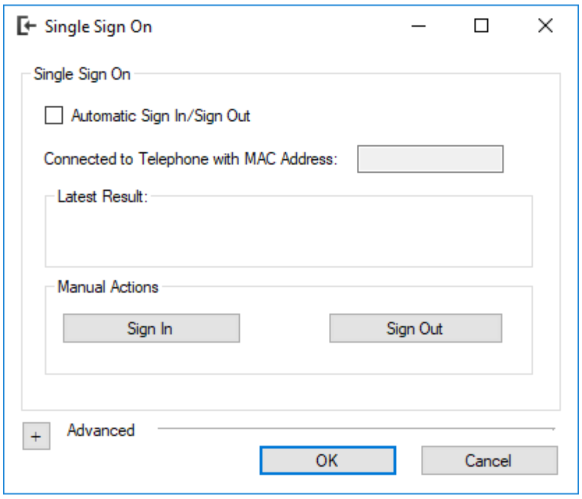


Figure 9-4 Single Sign On screen

The screen contains the following items:

Automatic Sign In/Sign Out

Check this checkbox to be automatically signed in when you log on in Windows, connect to the LAN or dock the PC. If you don't want to use Single Sign On always, uncheck the checkbox and use the 'Manual Actions' to sign in or sign out.

Connected to Telephone with MAC Address

In this field the program reports the ID of the telephone terminal that is used for connection of the PC to the LAN.

Latest Result

Latest result of sign in/sign out actions.

Manual Actions

To sign in or sign out your telephone terminal on request.

Advanced

Click on the '+' button to open the Advanced tab.
If you have more than one Network Interface Card, here you can select the one you want to use.

9.2.2.3. Call Handling TSP Configuration

First of all you also have to configure BCT server to use *Integrated Windows Authentication*. See chapter 17 Appendix G – BCT USER AUTHENTICATION MODES.

In order to configure dialing from Microsoft Outlook Contact List you must use "NEC Call Handling Line" as the line when calling a contact. This option is set during installation. When you have used other dialer applications other lines may have been configured.

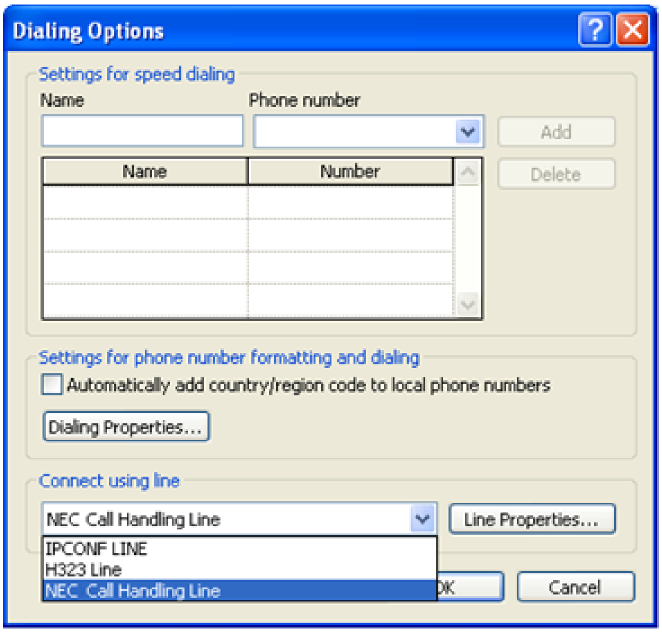
To configure the correct line:

1. Select a contact in Outlook and press the dial button in the toolbar. Or, use the menu **Actions > Call contact > New call**.

The **New call** dialog opens.

1. Press **Dialing Option…** to open the Dialing Options dialog.

2. In the drop down list for "Connect using line" select "NEC Call Handling Line" and press **OK**.



Connect using line: NEC Call Handling Line

Figure 9-5 Outlook dialing Options

3. On the client computer, leave the following settings of “Control Panel > Phone and Modem Options” empty:

   - “To access an outside line for local calls, dial:” and
   - “To access an outside line for long-distance calls dial”.

When left empty, the BCT server will automatically dial the correct access code when a call is made from Microsoft Outlook. If these values are filled with incorrect access codes (i.e. not matching the dialing rules of BCT), then the calls will fail. Therefore we recommend leaving these values empty.

9.2.1. Client Integration Troubleshooting

Problem:
When having configured IIS / CA on the server (i.e. Windows NT authentication + disable anonymous access) required for Microsoft Office or Internet Explorer integration, starting the BCT System Settings on the BCT server might result in a Windows logon dialog.

Solution:
Make sure that for current user the BCT URLs are seen as ‘Local intranet’. Typically this is being taking care of by the BCT server installation for the user running the setup. If logged on as a different user problem mentioned above can be solved by adding BCT server URL to “Local intranet” sites.

Note: *In general for trouble shooting it is recommended to install the diagnostic tooling. The installation package can be downloaded using "http://[business-connect-server]/bct/support/Diag@NetSetup.exe"*

9.3. Contact Center (Supervisor) Client - PC

This client software contains the BCT Supervisor Dashboard. The BCT Supervisor Dashboard is the application used by supervisors and administrators to setup and maintain the system. If the client is a supervisor, administrator client or wallboard client, execute this procedure.

The BCT Contact Center Client package will install some documentation files. Optionally, check for Acrobat Reader to be able to read this documentation. Installation of Acrobat Reader is offered via the **BCT DVD Main Menu**.

Installation Steps

1. Insert the BCT product DVD. The **BCT DVD Main Menu** window appears. If not, double click D:\Autorun.exe (where D is the drive letter of your DVD drive).

2. Under "Business ConneCT” click Contact Center (Supervisor) Client.

3. Now the “Choose Setup Language” selection dialog is shown. Note that this is only the installation language. Select the required language and click **OK**.

4. The Requirements Setup Wizard will pop up to perform a ‘System Configuration Check’ check, to determine if the client meets the installation requirements.

5. When all installation requirements are met, click **Next**.

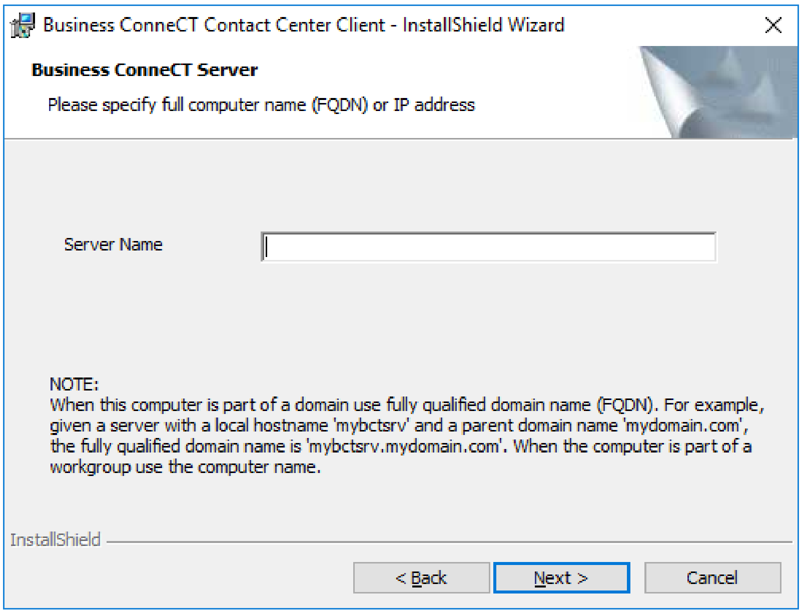
6. Next the Requirements Setup Wizard will pop up to ‘Install Prerequisites’, so it checks for required software and installs any missing items.

7. When asked to restart the system, click **Restart Now**. Wait until the PC is restarted and the installation continues.

8. The “Welcome”-window appears. Click **Next**.

9. The “Destination Folders”-window will appear. Choose the **Destination Folders** and click **Next**.

10. The “Business ConneCT Server”-window will appear. Enter the name of the BCT server. Read the help note about FQDN.



Business ConneCT Contact Center Client - InstallShield Wizard

Business ConneCT Server

Please specify full computer name (FQDN) or IP address

Server Name

NOTE:
When this computer is part of a domain use fully qualified domain name (FQDN). For example, given a server with a local hostname 'mybctsrv' and a parent domain name 'mydomain.com', the fully qualified domain name is 'mybctsrv.mydomain.com'. When the computer is part of a workgroup use the computer name.

Figure 9-6 Database location window

11. The “Ready to Install the Program”-window appears. Click **Install**.

12. The “Installing BCT Contact Center Client”-window shows the progress of the installation. When finished, click **Finish** to exit the installation wizard.

13. The Business ConneCT Supervisor Dashboard shortcut is made on your desktop and under ‘All Programs > Business ConneCT’.

Notes:

- When you upgrade also the SQL server location is requested. When you want the client to target another BCT server you can do this by changing the SQL location (that relates to this new BCT server).
- On a client computer, you can generate reports. To preview reports, you must define a printer. Simply configure a printer (recommended is the HP600 printer), there is no need to connect a real printer to the computer if printer output is not required.

9.3.1. Contact Center (Supervisor) Client troubleshooting

When at login of the Supervisor a message is shown with:

- Unable to contact the Business ConneCT server.
  Please contact your System Administrator.

Or

- An authentication error has been encountered:
  An unsecured or incorrectly secured fault was received from the other party.
  See the inner FaultException for the fault code and detail.

And when also in Diag@Net 'System.ServiceModel.Security.MessageSecurityException' is shown, make sure that the date/time is synchronized with the BCT server.

9.4. Soft Wallboard - PC

The BCT Soft Wallboard solution consists of a Soft Wallboard (SWB) client and a server component. The server component is always installed as part of the BCT Server installation. The SWB Client needs to be installed separately and is described in this chapter.

***Note:** SWB Client may not be installed on the BCT Server itself but only on a separate SWB Client PC!*

The BCT SWB Client is based on Microsoft PowerPoint, so before actually installing the BCT SWB Client software make sure that the following prerequisites are met:

- PC with Windows installed (32/64 bits mode)
- Microsoft PowerPoint 2013, 2016, 2019 or Office365 installed (32/64 bits mode)
  The SWB Client requires the Visual Basic for Applications (VBA) component to be installed with Microsoft Office.
- *Optional:* Microsoft *Excel 2013, 2016, 2019 or Office365 (for* Microsoft *Chart objects only)*

9.4.1. Soft Wallboard Installation

To install the BCT SWB Client software the following steps are required:

1. Ensure that the described prerequisites are met and that Microsoft PowerPoint is not running

2. Insert the Business ConneCT installation DVD; the Business ConneCT installation options should appear automatically (if not, browse the DVD driver for Autorun.exe and launch it manually)

3. Click the Soft Wallboard item to start the installation

4. Follow the wizard steps until the wizard successfully completes

5. After installation, check out the wallboard sample presentations (by default installed in *C:\Program Files (x86)\NEC\BCT Soft Wallboard\Samples*

For more information on how to configure the SWB Client please refer to BCT Administrator Guide.

9.5. Mobile Client – Smart Phone

9.5.1. Mobile Client Configuration

The BCT Mobile Client is the BCT Client that runs on a Mobile Smart Phone.

Because the BCT Mobile Client runs in an internet browser, minimal configuration is required on the Mobile Phone:

- Ensure that the browser allows the use of cookies. You can check this on your mobile phone as part of the internet browser settings or as part of the security settings.
- Also ensure that your mobile device supports GPRS-A, UTMS (3G) or HSDPA (3.5G) connections, and that these options are not prohibited at your connection settings.
- Make sure to have Java scripting enabled on your mobile phone

- Caching of html pages is not required but will considerably improve the performance when supported. If you can configure this at your browser, you are advised to allow caching.
- For easy access, define the BCT Mobile Client application as a favorite, as home page, or put it on desktop (iPhone).

9.5.2. Mobile Client Verification

To test the installation:

1. Create and configure a user as described in 8.1.13 BCT Mobile Client application and configure his mobile phone according to this chapter 9.5 Mobile Client.

2. On the Mobile Phone, start the internet browser and browse to the BCT Mobile Client Web Site: http://[domain name]/M , for example: http://bct.alholidays.com/M

3. Login with username and password (BCT Basic Authentication).

4. Browse through the screens and check the main functionality.

9.5.3. Mobile Client Troubleshooting

Problem: After each page access I have to login again

Solution: Your browser does not support cookies, or they have been prohibited. Change your browser settings on your mobile device to allow cookies.

Problem: I only get a login screen

Solution: Your browser does not support cookies, or they have been prohibited. Change your browser settings on your mobile device to allow cookies.

Problem: I cannot change the presence settings

Solution: You probably do not have the permission to change the presence settings. In this case, you cannot change your presence in the Desktop Client either. This permission can be configured in BCT System Settings user configuration page.

Problem: I have the proper permissions but I still cannot change the presence settings

Solution: You are probably logged into Desktop Client as Agent or Operator. If you are in one of these states, you are not allowed to change the presence settings.

Problem: No extension status shown

Solution: Presence must be manually switched on. Open the configuration file C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config and set the next value:

```
<directory.service>
  <add key="directory.service.presence.algorithm" value="BCTOnly" />
</directory.service>
```

After saving the file, a reboot of the BCT server is required

9.5.4. Mobile Operator Voicemail

There may be situations where the Mobile Operator’s voicemail system will answer a call before the call could be re-routed back to the BCT Operator or BCT Voicemail. This can be a result of user actions on the phone or a difference in for example CFNA timeouts in the PBX versus the Mobile Operator network.

The BCT and PBX configuration will make sure that all incoming DDI calls will follow the configured DDI fail routing options and/or BCT presence settings.

The “ignore”/”reject” function on a Mobile phone will forward a ringing call to the Mobile Operator’s voicemail system instead of the BCT Operator or BCT voicemail.

In order to avoid this from occurring either:

1. Switch Mobile phone voicemail off

2. Don’t select the “ignore”/”reject” function when a call is received on the Mobile phone and allow the Mobile phone to ring

In case a user initiates a call via the BCT Mobile Client UI first a call is setup from the PBX towards the user’s Mobile phone. In this case it is also possible to press the “ignore/reject” button, which will result in the call being forwarded to the Mobile operator’s voicemail. As soon as the Mobile operator’s voicemail answers, the second part of the call setup is executed, being the call towards the called party. This is of course an unwanted situation and can be avoided as indicated below:

1. Switch Mobile phone voicemail off

2. Don’t select the “ignore”/”reject” function when a call is received on the Mobile phone and allow the Mobile phone to ring

3. On SV8100/SV9100: Configure the Mobile Extension (ME) in such a way that a BCT Mobile Client user must press the ‘*’ as Connect Confirmation to accept the call. Only after confirmation a call is setup to the called party is performed by BCT/SV8100/SV9100. This call setup confirmation function will avoid the call scenario as described above. See also 4.4.4 Mobile extension setup for BCT Mobile Client

9.6. BCT Agent – Smart Phone

With the NEC BCT Agent App a Business ConneCT Contact Center Agent can login and control their Ready/Not-Ready state from a Smart Phone. Agents can make themselves available to receive customer calls on their mobile phone from anywhere on the mobile network.

Smart Phone App installation:

- Android: install “NEC Business ConneCT Agent” from the Google Play Store.
- iOS: install “NEC Business ConneCT Agent” from the Apple App Store.

The BCT Agent App connects to the BCT Server via port 32011 (default and secure).
The connected port should be reachable by the Smart Phone.

Note: Don’t use Mandarory Call Type for agents using the BCT Agent App.

9.7. XML Client – DT Terminal

Installation

The BCT DT XML solution is part of the default BCT Server installation. When the BCT server installation is finished then all the relevant components for the XML applications are installed and ready to use.

Preconditions

- XML Client Employee:
  It is required that BCT User Accounts are created (username & password, BCT basic authentication) with the 'Employee' role assigned (make sure you have enough Employee licenses available) so users can logon to the BCT DT XML Employee on their desktop phone.
  TIP: use uppercase character passwords to avoid changing input modes at the terminal before entering passwords.
  See chapter 9.7.6 XML Terminal – "Employee, Agent and Directory Browser" Mode for selection.
- XML Client Agent:
  It is required that BCT User Accounts are created (username & pin code, BCT basic authentication) with the 'Phone Based Agent' role assigned (make sure you have enough Phone Based Agent licenses available) so users can logon to the BCT DT XML Agent on their desktop phone. See chapter 9.7.6 XML Terminal – "Employee, Agent and Directory Browser" Mode for selection.
- Use latest available terminal firmware version.
- Check **BCT Boundary Specification** for supported terminal type.

Configuration of terminal

In order to be able to access the BCT DT XML on a DT terminal some settings on the terminal need to be performed. Configuring these terminal settings can be done in three different ways:

1. for each terminal on the terminal itself (administrator menus)
2. for each terminal via a Web browser (note: can be disabled in the terminal)
3. for multiple terminals at once via an 'IP Phone Manager'.

Note: *pre-condition is that the -to be configured- XML- terminals have been configured correctly in the PBX and are operational.*

9.7.1. DT NSIP XML terminals connected to SV PBX

Configure non-default settings via Web progamming:

1. Fill in terminal IP-address in the address field of the web browser.

2. Login as "ADMIN" with password (default password: 6633222)

3. Security Push Server

   - Push Server Access > select 2. Enable

   - Client IP Address > Client 1 > fill in IP-address of BCT Server

4. Application Settings XML Settings

   - Terminal ID > fill in the extension number.
     This Terminal ID is used for authentication and authorization of a user.
     It is required that the configured Terminal ID is:
     - Identical to the actual terminal DNR as configured for this terminal in the PBX
     - Identical to the terminal DNR as configured in the BCT User Account for the user of this terminal

   - XML Browser > Home URL > fill in http://<BCTserver>/XmlDirectory/default.aspx

   Note: *It is important that the terminal can resolve the BCT server name in the network otherwise use the BCT Server IP-address*

5. Application Settings Popup Popup Mode

   - Select 1 Enable

6. Save settings. The Terminal restarts with the new settings.

9.7.2. DT Std. SIP XML terminals connected to iS3000 PBX platforms/SIP@Net or UNIVERGE 3C

Note: *In the text below, items between [] need to be replaced with the actual data!*

1. Open the DT-[MAC-address]-phone.cfg configuration file in an XML editor.
   You can find this file on the TFTP server in the LAN network.

2. Locate the <DT_PHONE_CONFIG_DATA> and </DT_PHONE_CONFIG_DATA> parameters.

3. Add the following lines between the tag names **<DT_PHONE_CONFIG_DATA>** and **</DT_PHONE_CONFIG_DATA>**:

```
<DT_PHONE_CONFIG_DATA>
  <DT_LINE_DATA
    line.1.extension="[Phone Number]"
    line.1.displayname=""
    line.1.maxcalls="3"
    line.1.primary.address="[SIP server | IP address]"
    line.1.primary.port="5060"
    line.1.outboundproxy.address=""
    line.1.outboundproxy.port=""
    line.1.authentication.username=""
    line.1.authentication.password=""
  />
  <DT_SIP_DATA sip.reg.expiry="300" sip.transport="1" />
  <DT_PHONE_DATA
    phone.voicemail.extension=" "
    phone.http.useragent.id="1"
  />
  <DT_PHONE_SECURITY_DATA
    security.push.access="1"
    security.push.server.address="[BCT Server IP address]" />
  <DT_HOME_URL phone.home.url="http://[BCT server IP
address/hostname]/XmlDirectory/default.aspx" />
</DT_PHONE_CONFIG_DATA>
```

4. When the changes are made and the configuration file is saved reboot the terminal to force the download of this configuration file.

9.7.3. When making use of the selection menu (SV8100/SV9100 only)

When the XML terminals have also other XML servers, the SV8100/SV9100 can provide an option menu, from which a user can select the desired XML application.

Use Terminal Programming, WebPro or PCPro and program 10-56 and fill in:

Name: BCT
URL: http://<BCTserver>/XmlDirectory/default.aspx

Replace XML Browser Home URL with http://<PBXaddress>/apps.htm.
The XML terminal now points to the selection menu of the SV8100/SV9100.

9.7.4. XML terminal configuration – multiple terminals in parallel via management application (IP Phone Manager)

More information can be found in the documentation of the IP Phone Manager.

Note that the Terminal ID is specific for every terminal. For checking correct working of the XML application please refer to paragraph 9.7.5 How to access BCT DT XML client.

The BCT User Guide gives information about the provided functions.

9.7.5. How to access BCT DT XML client

Depending on the terminal type, the BCT DT XML can be accessed in the following ways:

- Long press Home key
- Feature button (Std SIP terminals only)
- Home softkey via Menu key
- Menu key, Tool and Service

Note: *To exit the BCT DT XML , simply press the exit key (hard key). Note that when the client was not logged out before exiting, the client remains logged in even though the terminal is no longer in XML mode. So the next time the BCT DT XML is accessed, no log in is needed.*

9.7.6. XML Terminal – "Employee, Agent and Directory Browser" Mode

The XML Client can operate in 3 different modes:

1. Employee mode (default setting) with ‘BCT’ authentication type.
2. Agent mode with ‘BCTAgent’ authentication type.
3. Directory Browser mode with ‘None’ authentication type. No login is required and only the Directory Browser functionality of the Employee is offered.

The XML Client mode selection is a system-wide option. No mixed configuration is possible.

To change the mode:

1. Open the Configuration Manager and select the configuration file ‘C:\Inetpub\wwwroot\XML Directory\web.config’.

2. Locate the key: AuthenticationType

3. Change the value to eiher ‘BCT’, ‘BCTAgent’ or ‘None’
4. Press button Save to store the value.

9.7.7. XML Client Agent settings

XML Client Agent settings can be defined by open the Configuration Manager and select file “C:\Inetpub\wwwroot\XML Directory\web.config”.

Settings are:

1. Select the BCT Client in Agent mode by changing key AuthenticationType to value BCTAgent.
2. The way numbers are translated to names can be defined. See chapter 8.5.15 Number to name translation for details.
3. An Agent can have one or more Routers. The Router with the highest number of calls in the queue can trigger a color indication in the message waiting Led. When no calls queued the Led is off.
   When 1 till QueueMinorThreshold calls in queue the Led will flash green for 3 seconds.
   When QueueMinorThreshold till QueueMajorThreshold calls in queue the Led will flash yellow for 3 seconds.
   When QueueMajorThreshold or more calls in queue the Led will flash red for 3 seconds.
   The usage and switching of the LED can be defined by changing the value of the following keys:
   ShowGreenLed: value True for using the green LED; value False for not using the green LED.
   ShowYellowLed: value True for using the yellow LED; value False for not using the yellow LED.
   ShowRedLed: value True for using the red LED; value False for not using the red LED.
   QueueMinorThreshold: set value to required threshold level. Default value is 3. Minimum value is 2.
   QueueMajorThreshold: set value to required threshold level. Default value is 5. Minimum value is QueueMinorThreshold +1.
4. The Agent Status Page and Queue Led indication can be refreshed automatically. Default value is 30 seconds. The Minimum value is 10 seconds. Increase the Agent auto refresh interval when XML Agent takes too much system resources in IIS. To change the refresh time change the value of key AgentAutoRefreshInterfal to the required time.
5. On startup of the Login menu the Initial State for Login is Not Ready. This can be changed to Ready by setting key InitStateReady to value True.

9.7.8. Secure XML Terminal

DT XML Terminal		**BCT XML running in IIS**
Client	------ HTTP port 80 or HTTPS port 443 ----->	Server
Push Server	<---- HTTP port 82 or HTTPS port 8282 -----	Push Client
	not-secure or secure	

Default is the not-secure HTTP operation.
The secure XML HTTPS can be selected by programming the home URL of the DT terminal to: “**https**://[BCT server hostname]/XmlDirectory/default.aspx".

By default the BCT XML server makes also the Push Client secure when a secure home URL is received.
Check the DT Terminal documentation and the BCT Boundary Specification for secure XML support.
A certificate is required for the DT terminal to perform certificate authentication when receiving a secure Push.

9.7.8.1. Certificate for the secure Push Server

For the secure Push operation, a certificate must be loaded in the DT Terminal and the BCT Server PC.
Follow the chapter Certificate Creation in the DT Resource Manual issue 13.0 or later.

With the OpenSSL tool (Prerequisite) it is possible to create certificates as described in section STD-SIP Push Function.
Create a Root Certificate (rootcert.pem) and a Server Certificate (servercert.pem).
Follow section Common Certificate Creation to have a common certificate for all terminals.
Convert the rootcert.pem to rootcert.der with:

```
> openssl x509 -outform DER -in rootcert.pem -out rootcert.der
```

Copy the created servercert.pem to the terminal (TFTP) boot server.
Copy the created rootcert.der to the BCT server.
Executing rootcert.der on the BCT server: press Install Certificate…, select Local Machine, press Next, select Place all certificates in the following store, press Browse, select Trusted Root Certificate Authorities, press OK, press Next and press Finish.

9.7.8.2. Program example of a DT900 St. SIP terminal with secure XML

Contents of file dt-6ce4daf1616b-phone.cfg:

```
<?xml version="1.0" encoding="utf-8"?>
<DT_PHONE_CONFIG_DATA>
 <DT_LINE_DATA
  line.1.extension="1080"
  line.1.displayname="U1080"
  line.1.maxcalls="1"
  line.1.primary.address="192.168.12.203"
  line.1.primary.port="5060"
  line.1.outboundproxy.address=""
  line.1.outboundproxy.port=""
  line.1.authentication.username=""
  line.1.authentication.password=""
 />
 <DT_SIP_DATA
  sip.reg.expiry="300"
  sip.transport="1"
 />
 <DT_PHONE_DATA
  phone.voicemail.extension=""
  phone.show.registration.name="0"
 />
 <DT_PHONE_SECURITY_DATA
  security.8021x.enable="0"
  security.8021x.username=""
  security.8021x.password=""
  security.push.server.port="82"
  security.push.https.server.cert="servercert.pem"
  security.push.access="3"
  security.push.server.https.port="8282"
  security.push.server.address="172.29.126.176"
 />
 <DT_HOME_URL phone.home.url="https://DESKTOP-9G9ALPP/XmlDirectory/default.aspx" />
</DT_PHONE_CONFIG_DATA>
```

Replace environment specific DT_LINE_DATA and DT_PHONE_SECURITY_DATA.
The BCT server hostname must be known in the DT terminal network.
When changing from HTTP to HTTPS: log out the DT XML terminal user before rebooting the DT terminal to get the new configuration.

9.7.8.3. Disable or change the Secure Push Url format

Disable of secure Push XML is needed when the home URL is programmed for the secure HTTPS operation and your DT Terminal does not support secure Push XML.

Open the Configuration Manager and select file “C:\Inetpub\wwwroot\XML Directory\web.config”.
To disable change the SecurePushUrlFormat:

```
   <add key="SecurePushUrlFormat" value=""/>
```

The default push server https port is 8282 as programmed in the dt-<mac-address>phone.cfg file.
When changed also change this in the SecurePushUrlFormat.

```
   <add key="SecurePushUrlFormat" value="https://{0}:8282/cgi/Push.cgi"/>
```

Note that SecurePushUrlFormat is a system wide option for all connected DT XML terminals.

9.7.9. XML Terminal troubleshooting

Problem: No extension status shown

Solution: Presence must be manually switched on. Open the configuration file C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config and set the next value:

```
<directory.service>
 <add key="directory.service.presence.algorithm" value="BCTOnly" />
</directory.service>
```

After saving the file, a reboot of the BCT server is required.

9.8. UC Connector – PC

The ‘UC Connector’ package integrates with 'Skype for Business' and offers call support with NEC IP based PBX systems.

It can be installed via the option called "UC Connector" offered by the BCT autorun.exe application (started via auto play of DVD - if not automatically started do run D:\Autorun.exe - where D is DVD drive letter). For details please check the “UC Connector” Installation Guide available on the BCT DVD.

9.9. Salesforce Open CTI Adapter – PC

The ‘Salesforce Open CTI Adapter’ package offers agents communication and Contact Center features fully embedded within the Salesforce.com solution.

It can be installed via the option called "Salesforce Open CTI Adapter" offered by the BCT autorun.exe application (started via auto play of DVD - if not automatically started do run D:\Autorun.exe - where D is DVD drive letter). For details please check the “Salesforce Open CTI Adapter” Installation Guide available on the BCT DVD.

10. BACKUP AND DATABASE MAINTENANCE

A good backup plan can mean the difference between a complete re-installation or restore that takes a few minutes:

- Always make an image of a fully operational system. Do this again after a software upgrade.
- Back up the database regularly, and after major configuration changes.
- Create the scheduled jobs for the database using the Runtime Manager.
- Explain to the customer the maintenance tasks described in this chapter and find out how these tasks can become part of their daily routine

10.1. Hard disk image

Make a hard-disk image of the system using software from Acronis, Ghost or any other imaging tool. This image can be stored on a separate partition, a network drive, a detachable device, etc. Make sure you have a ‘fire copy' - a copy stored at another geographical location.

Most imaging tools let you run imaging software from a bootable CD and create an image of the server during normal operation. You can also schedule this action, preferably outside business hours to prevent additional load on the server.

Some imaging tools can create an image remotely using a Backup Manager. These tools install an Imaging Agent Service on the BCT server. When the Backup Manager requests it, the service creates an image.

A hard-disk image is a snapshot of that moment. All subsequent changes are lost once the image is restored. If this is unacceptable for the customer, you can either make images more frequently, or create database backups, or both.

Some customers use a RAID system. The server has more than one hard-disk and if the hard-disk crashes the other disk(s) take over. In this case you must still make disk images. A RAID system is not capable of restoring a corrupted system.

10.2. Database backup and maintenance

WARNING: *If you do not maintain the database, the system performance will degrade over time. Eventually, the database server will run out of disk space!*

You must backup and maintain the BCT database. A database backup contains BCT's configuration and call data. Every application based on a database will grow until it runs out of disk-space.

Note: In case you want to shrink the transaction logfile, use Microsoft SQL Server Management Studio, on the United database, context menu 'Tasks', 'Shrink', 'Files' and select File type: Log.

To backup the database, use the BCT Runtime Manager. You can create and schedule backups. See section 10.3 Database Maintenance using Runtime Manager. Note that the Runtime manager can only make backups of the local database that is installed on the BCT Server.

In case the database is not local on the BCT server, but on a remote SQL server, we recommend to use Microsoft SQL Server Management Studio for database backup and restore.

If the BCT configuration is fixed and there is no serious demand for reporting, unscheduled database backups are sufficient.

Keep in mind that the BCT database contains other information besides call data. It contains the client's personal information like the presence information, the personal directory, the Email and home address information, and so on. If this information is valuable to the customer, you must make regular backups.

For immediate database maintenance actions you can also use the OSQL command line utility.

10.3. Database Maintenance using Runtime Manager

BCT comes with an SQL Maintenance plan to perform basic maintenance tasks. The scheduled jobs required for maintenance are not created by default any more. They can be created and updated by using the Runtime Manager. The jobs are enabled by default after creation or update. When you want to (temporarely) prevent execution of the maintenance jobs they can be disabled in the Runtime Manager. To execute the jobs the 'SQL Server Agent' service should be running.

SQL Server Express does **NOT** include an SQL agent, so the SQL Maintenance plan will **NOT** be available. For database maintenance for SQL Express installations see section 10.4 Database Maintenance for SQL Express.

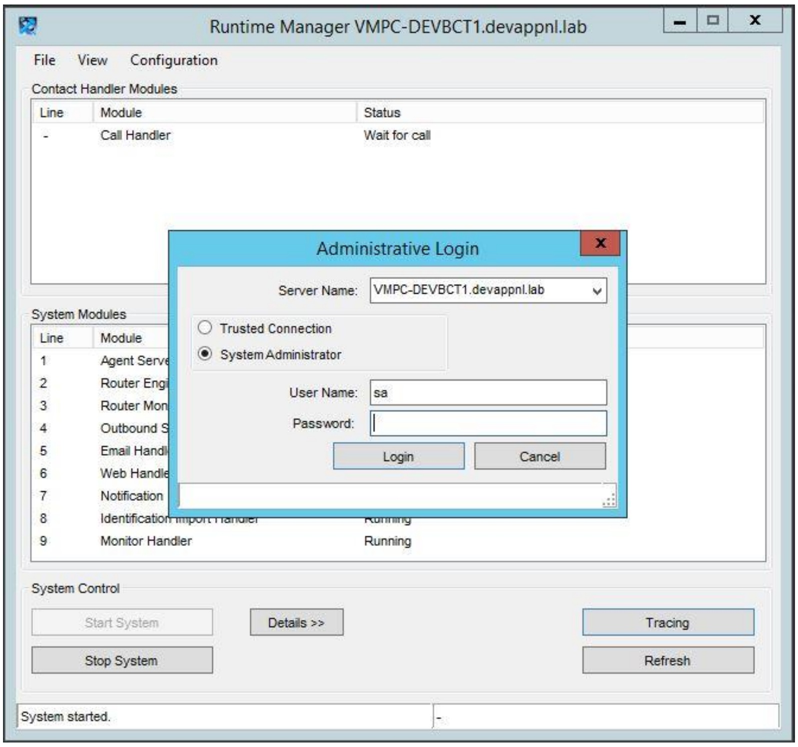
Also be aware that when jobs are enabled, the files are generated on the server. Eventually the hard disk will fill up completely, so make sure you archive this folder regularly. Possible jobs include:

- Complete database backup once a day - at 12:00 AM
- Database integrity check once a week - Sunday 12:00 AM
- Transaction log backup every hour for every working day

To create or update the database maintenance jobs:

1. Open the Runtime Manager
2. Select **Configuration** and **Database**

3. The system asks for the username and password to login to the SQL server. This user must have permission to create backups, for example the user “sa”.



Line	Module	Status
-	Call Handler	Wait for call

Line	Module	Status
1	Agent Serve	
2	Router Engi	
3	Router Mon	
4	Outbound S	
5	Email Handl	
6	Web Handle	
7	Notification	
8	Identification Import Handler	Running
9	Monitor Handler	Running

Server Name: VMPC-DEVBCT1.devappnl.lab

○ Trusted Connection

● System Administrator

User Name: sa

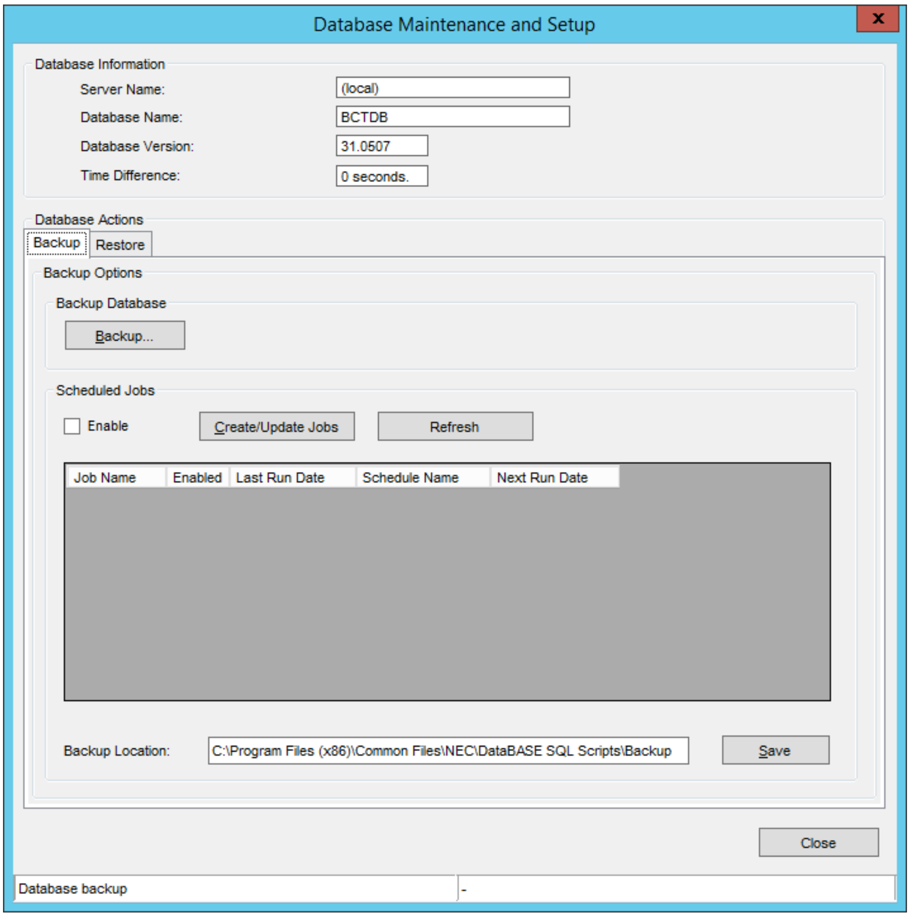
Password:

System started.

-

Figure 10-1 Runtime Manager Login

4. After login, the Database Maintenance and Setup window is shown.
The first time after installation there are no maintenance jobs yet:



Database Maintenance and Setup

Database Information

Server Name: (local)

Database Name: BCTDB

Database Version: 31.0507

Time Difference: 0 seconds.

Database Actions

Backup | Restore

Backup Options

Backup Database

Scheduled Jobs

☐ Enable

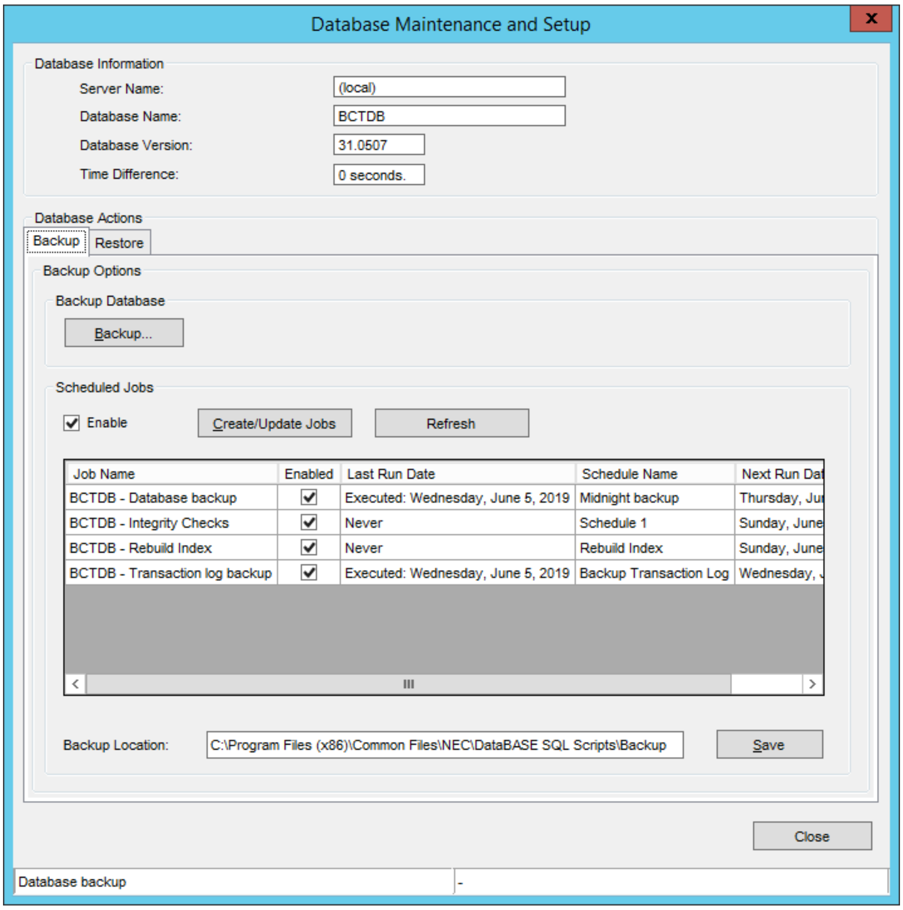
Job Name	Enabled	Last Run Date	Schedule Name	Next Run Date

Backup Location: C:\Program Files (x86)\Common Files\NEC\DataBASE SQL Scripts\Backup

Database backup | -

Figure 10-2 Runtime Manager DB Maintenance and Setup Initial window

5. Click “Create/update jobs” to create the database maintenance jobs. The jobs are enabled by default after creation.



Server Name: (local)

Database Name: BCTDB

Database Version: 31.0507

Time Difference: 0 seconds.

☑ Enable

Job Name	Enabled	Last Run Date	Schedule Name	Next Run Dat
BCTDB - Database backup	☑	Executed: Wednesday, June 5, 2019	Midnight backup	Thursday, Ju
BCTDB - Integrity Checks	☑	Never	Schedule 1	Sunday, June
BCTDB - Rebuild Index	☑	Never	Rebuild Index	Sunday, June
BCTDB - Transaction log backup	☑	Executed: Wednesday, June 5, 2019	Backup Transaction Log	Wednesday, .

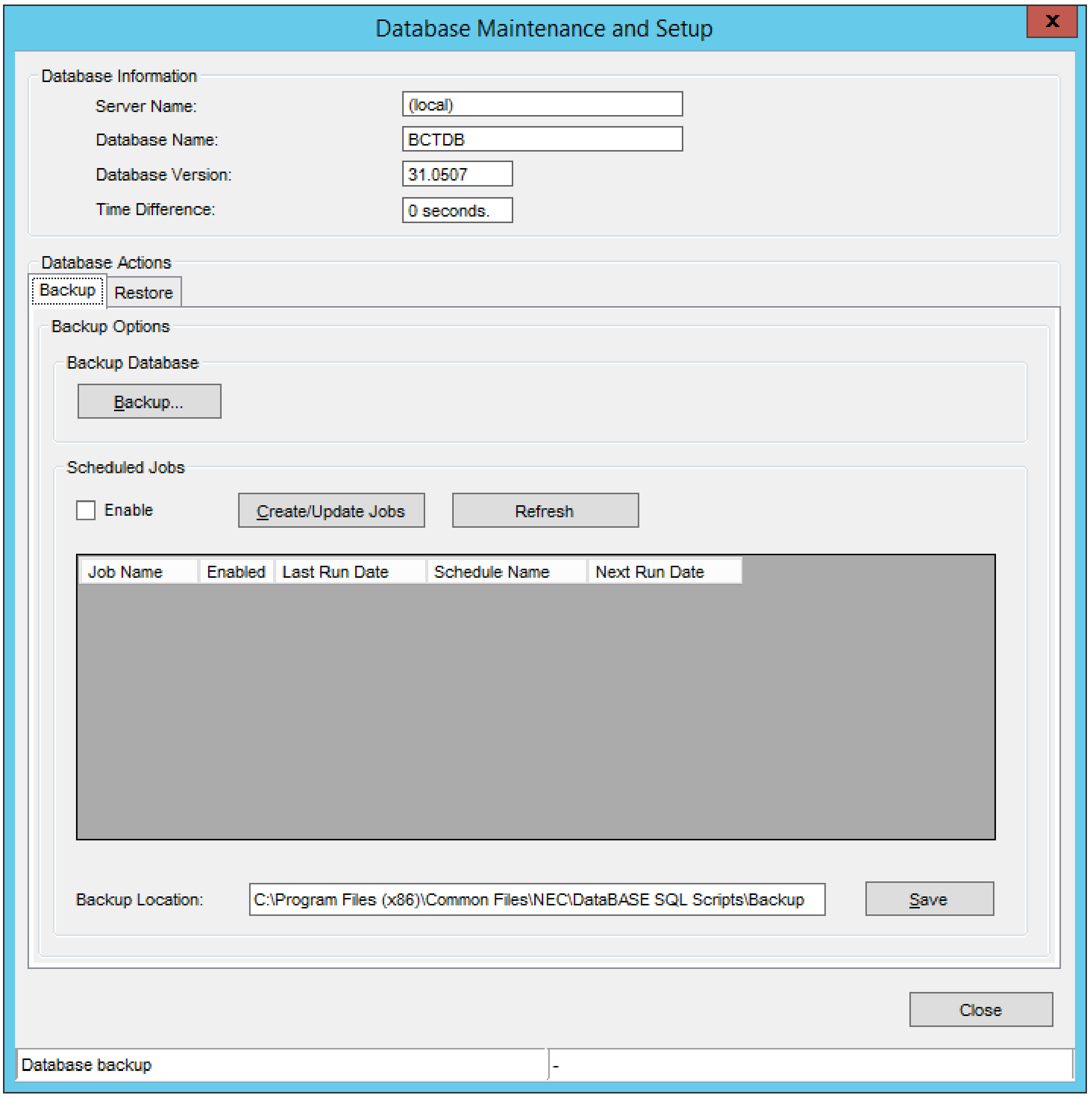
Backup Location: C:\Program Files (x86)\Common Files\NEC\DataBASE SQL Scripts\Backup

Database backup | -

Figure 10-3 Runtime Manager DB Maintenance and Setup window

6. To update the maintenance jobs after an upgrade click “Create/update jobs”. This will recreate the maintenance jobs.

7. To prevent execution of the maintenance jobs uncheck the "Enable scheduled jobs" option. Now all jobs will be disabled. It is also possible to disable individual jobs.
   Jobs can be enabled again in the same window.



Database Maintenance and Setup

Database Information

Server Name: (local)

Database Name: BCTDB

Database Version: 31.0507

Time Difference: 0 seconds.

Database Actions

□ Enable

Job Name	Enabled	Last Run Date	Schedule Name	Next Run Date

Backup Location: C:\Program Files (x86)\Common Files\NEC\DataBASE SQL Scripts\Backup

Database backup | -

Figure 10-4 Runtime Manager DB Maintenance and Setup window – SQL Express

In Figure 10-4 Runtime Manager DB Maintenance and Setup window – SQL Express scheduled backups are disabled.

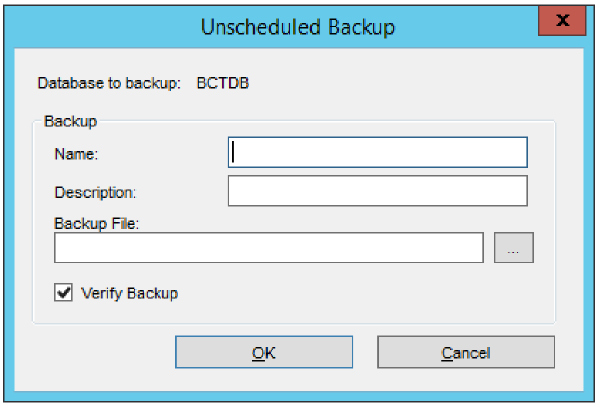
To create an unscheduled complete backup:

1. Open the Runtime Manager

2. Select **Configuration** and **Database**

3. The system asks for the username and password to login to the SQL server. This user must have the rights to create backups, for example the user “sa”.

4. Click "Unscheduled backup", the Unscheduled backup window is now displayed.



Database to backup: BCTDB

☑ Verify Backup

Figure 10-5 Database Maintenance and Setup – Unscheduled Backup window

5. Now follow the next steps to create a backup

- Select radio button "Database Complete" (default)
- Insert Name and Description
- Check mark "Verify backup" (default)
- Choose a backup location and click **OK**

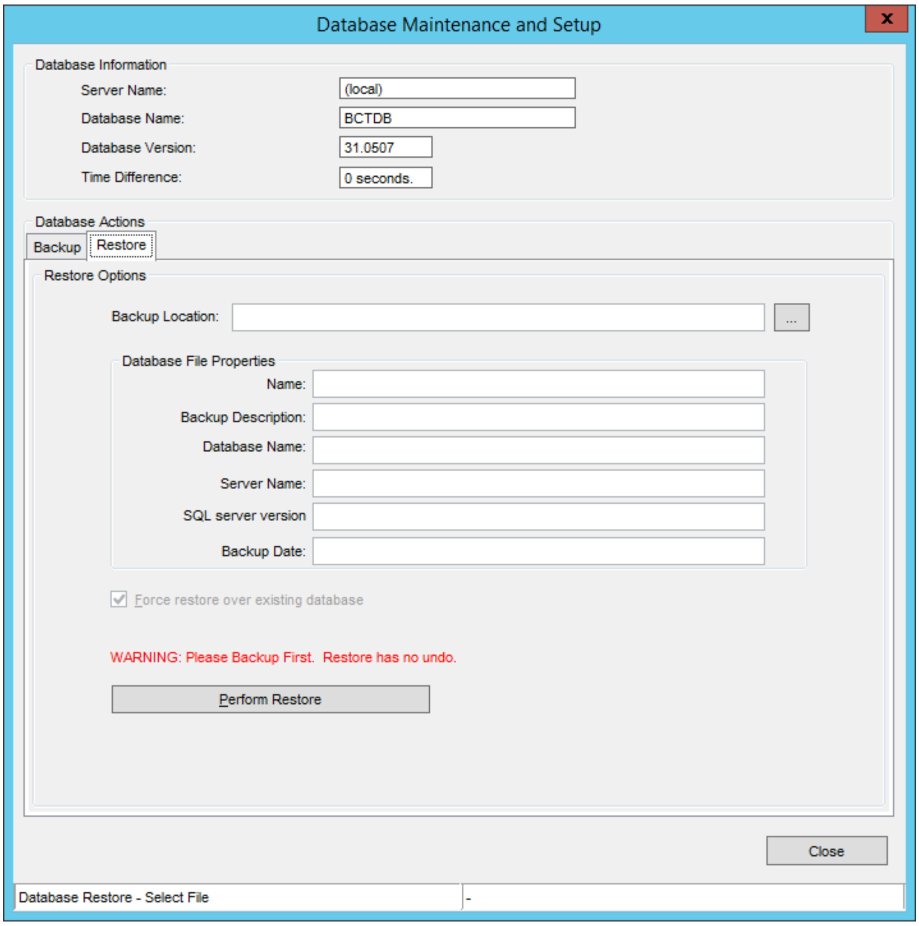
To restore a database full backup:

WARNING*: Only restore a database made on the same BCT Server and from the same BCT version.*

1. Start the Runtime Manager, select Configuration and Database, the system asks for the username and password to login to the SQL server.

2. Goto the restore tab and select the backup file.

3. Press the "Perform Restore" button.



Server Name: (local)

Database Name: BCTDB

Database Version: 31.0507

Time Difference: 0 seconds.

☑ Force restore over existing database

WARNING: Please Backup First. Restore has no undo.

Database Restore - Select File | -

Figure 10-6 Database Maintenance and Setup - Restore Backup window

Now all NEC services will be stopped, the database will be restored and all services will be restarted in an orderly fashion. The system will become fully operational with the restored backup.

Note: *In case you are using a 3rd party tool to restore the database, you can stop and start all services manually. Start the Runtime Manager. The main window opens. Click on "<< Details". A subwindow opens, containing buttons to Stop All Services or Start All Services.*

10.4. Database Maintenance for SQL Express

SQL Server Express does **NOT** include an SQL agent, so the SQL maintenance shall be done in a different way.

We recommend a freeware database backup tool like “SQL Backup and FTP” (www.sqlbackupandftp.com) in order to schedule backups.

BCT monitors the database index fragmentation and when an index has an average fragmentation above 30% and the number of fragments exceeds 500 it shows a warning in the system health page. To maintain good performance of the databsae it is important to regularly rebuild the indexes. We recommend to use Microsoft SQL Server Management Studio for this job.
In the Management Studio, enter the script below and execute.

```
Use United
```

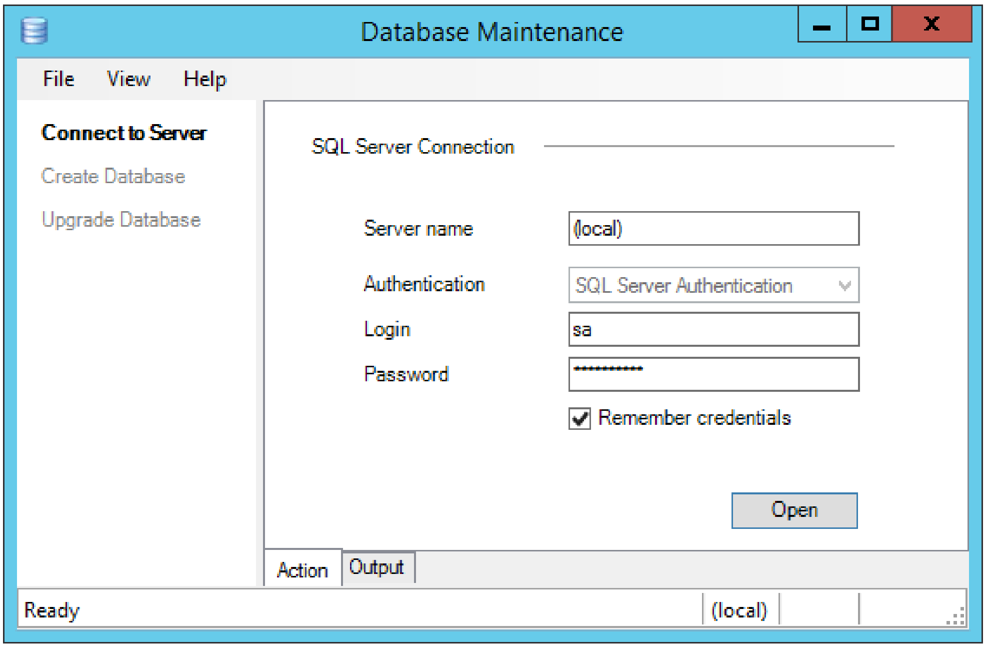
```
GO
EXEC sp_MSforeachtable @command1="print '?'",@command2="SET QUOTED_IDENTIFIER
ON;ALTER INDEX ALL ON ? REBUILD"
GO
EXEC sp_updatestats
GO
```

Note: *The 30% and 500 numbers used by BCT as a reference when deciding to show index fragmentation warning, are configurable in the Monitoring service config file via SqlMaxIndexFragmentationPercent and SqlMaxIndexFragmentsCount fields .*

10.5. Database Maintenance tool

If the SQL United database seems corrupt, or you want to start again with a fresh database, you don't need to re-install BCT. Instead, you can use the Database Maintenance tool. This application is by default in 'C:\Program Files (x86)\Common Files\NEC\DataBASE SQL Scripts' and is named 'Installer.Database.exe'.

When you start the application, the first step is to connect to the (current used) SQL database server. Click "Open" to establish the database connection. See also figure below:



Server name: (local)

Authentication: SQL Server Authentication

Login: sa

Password: ***********

☑ Remember credentials

Ready (local)

Figure 10-7 Database Maintenance – Connect to Server

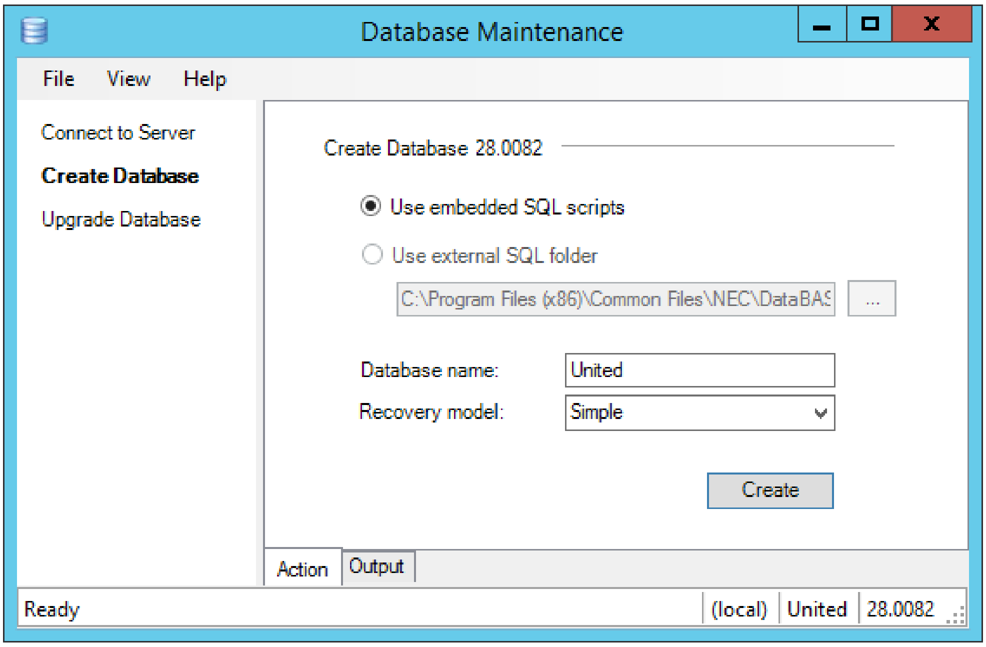
After the connection is established you are offered 2 options shown in the left pane:

- **Create Database.** Select this option and click "Create" to create a fresh 'United' database. In case it already exists (which obvious would be the case) you will be warned and asked if you want to replace it.

- **Upgrade Database.** Select this option and click "Upgrade" to upgrade (or repair) the database to get database to its latest scheme version. This preserves the table data but will recreate the SQL views and stored procedures. This option will also apply when you have restored a database of an older BCT version.

Note: *Typically it is recommended to first stop all BCT services (via the 'UCS Runtime Manager').*

Note: *For all above described options you can monitor its progress via the 'Output' tab-page.*



Create Database 28.0082

● Use embedded SQL scripts

○ Use external SQL folder

C:\Program Files (x86)\Common Files\NEC\DataBAS

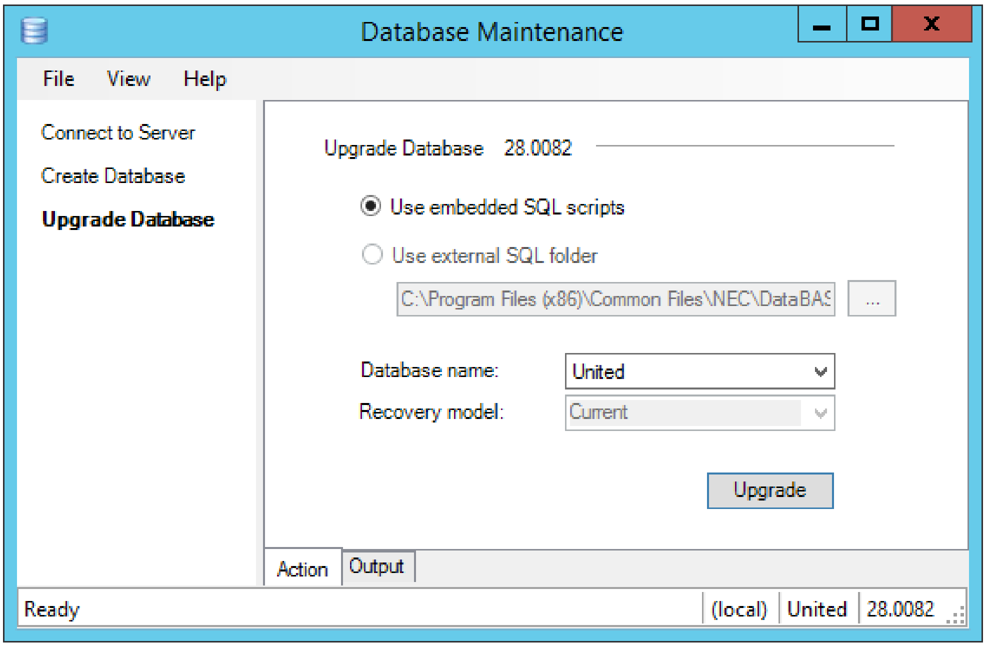
Database name: United

Recovery model: Simple

Create

Ready | (local) | United | 28.0082

Figure 10-8 Database Maintenance – Create Database



Upgrade Database 28.0082

● Use embedded SQL scripts

○ Use external SQL folder

C:\Program Files (x86)\Common Files\NEC\DataBAS

Database name: United

Recovery model: Current

Upgrade

Ready | (local) | United | 28.0082

Figure 10-9 Database Maintenance – Upgrade Database

10.6. How to save and limit the number of database backup files

You can create a batch job that copies the database backup files (.bak), keeps a variable number of previous backups files available, and deletes older versions.

Create a file (BCT_database_backup.bat) containing the following lines:

```
if not exist C:\Progra~1\Common~1\NEC\DataBA~1\backup\*.bak goto end
del D:\BCT_database_backup\day-5\*.bak
move D:\BCT_database_backup\day-4\*.bak D:\BCT_database_backup\day-5\
move D:\BCT_database_backup\day-3\*.bak D:\BCT_database_backup\day-4\
move D:\BCT_database_backup\day-2\*.bak D:\BCT_database_backup\day-3\
move D:\BCT_database_backup\day-1\*.bak D:\BCT_database_backup\day-2\
move C:\Progra~1\Common~1\NEC\DataBA~1\backup\*.bak D:\BCT_database_backup\day-1\
:end
```

This job:

- has to be executed via a scheduled task of Windows;
- expects the database backup files in the default folder;
- expects there is a partition D;
- expects you to create folders BCT_database_backup\day-x on the D: partition, where day-x can be the age of the backup file.

You can also use week-x, which depends on the scheduled task defined.

11. Appendix A - TROUBLESHOOTING

11.1. Checking System Health

BCT includes automatic health checks to help you ensure the system is running properly and anticipate possible problems before they affect users. You can also clearly see when the system is starting up (during which time it's normal for some functions not to be available). You can check system health from any computer, by logging in as administrator. A System Health page gives you one clear overview of the system's status.

To start System Health checks:

1. On the BCT server, choose:
   Start/Programs/Business ConneCT/Tools/System Health Status.

2. A System Health icon appears in the server's task bar and shows the system status.
   The icon is a BCT Logo without mark or with a yellow or red mark:

- All check results good (healthy);
- One or more checks failed (unhealthy);
- System starting up, some checks good.

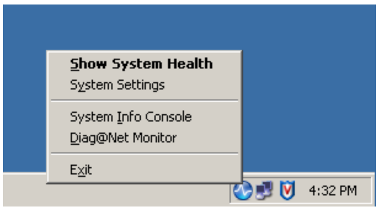


Figure 11-1 System Health taskbar icon and right mouse menu on BCT server

Note: *To make the health icon "always visible" in the task bar should be done manually.*

Note: *A notification is provided when the health status changes from Healthy to unhealthy.*

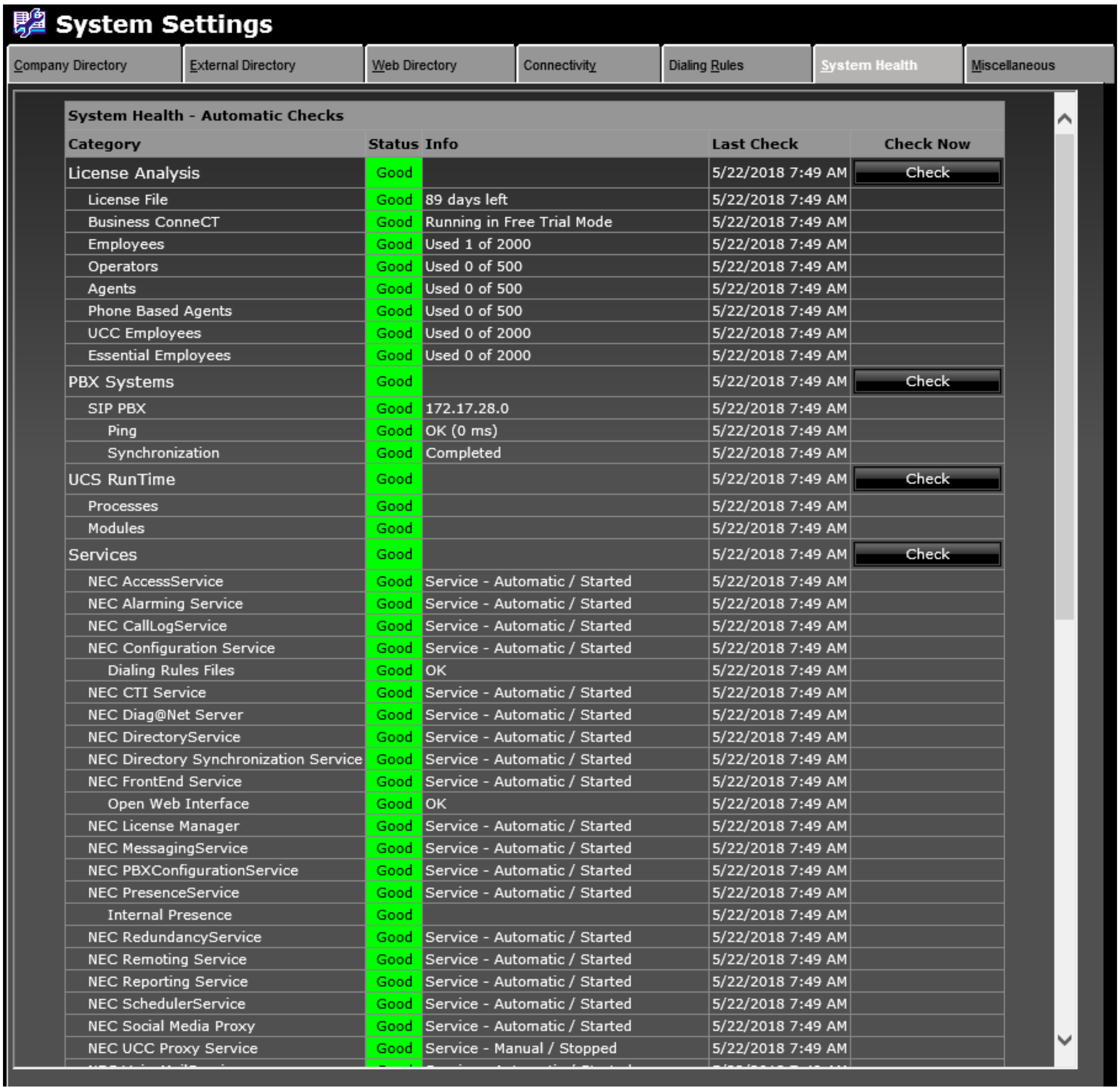
To check System Health remotely:

1. Log in as administrator and choose the System Health tab in BCT System Settings. The System Health page appears. See Figure 11-2 System Health page.

2. To request an immediate check for an item, click the Check Item button in the item's Check Now column, if available.

3. To test communication between the server and a PBX, you can:

   - Ping the PBX from the server;
   - Get, set or clear the Do Not Disturb state of an extension.

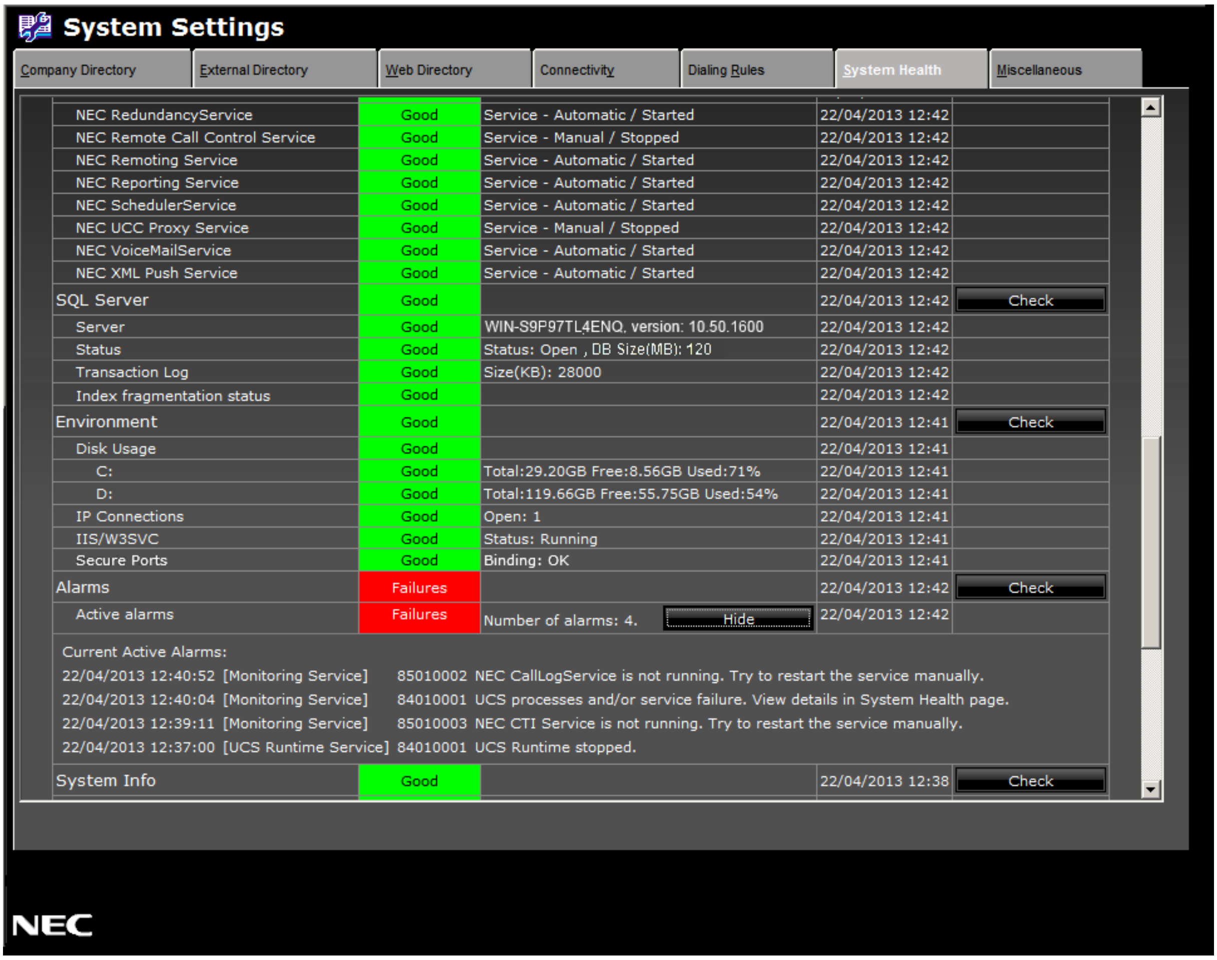


System Health - Automatic Checks

Category	Status	Info	Last Check	Check Now
License Analysis	Good		5/22/2018 7:49 AM	Check
License File	Good	89 days left	5/22/2018 7:49 AM	
Business ConneCT	Good	Running in Free Trial Mode	5/22/2018 7:49 AM	
Employees	Good	Used 1 of 2000	5/22/2018 7:49 AM	
Operators	Good	Used 0 of 500	5/22/2018 7:49 AM	
Agents	Good	Used 0 of 500	5/22/2018 7:49 AM	
Phone Based Agents	Good	Used 0 of 500	5/22/2018 7:49 AM	
UCC Employees	Good	Used 0 of 2000	5/22/2018 7:49 AM	
Essential Employees	Good	Used 0 of 2000	5/22/2018 7:49 AM	
PBX Systems	Good		5/22/2018 7:49 AM	Check
SIP PBX	Good	172.17.28.0	5/22/2018 7:49 AM	
Ping	Good	OK (0 ms)	5/22/2018 7:49 AM	
Synchronization	Good	Completed	5/22/2018 7:49 AM	
UCS RunTime	Good		5/22/2018 7:49 AM	Check
Processes	Good		5/22/2018 7:49 AM	
Modules	Good		5/22/2018 7:49 AM	
Services	Good		5/22/2018 7:49 AM	Check
NEC AccessService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Alarming Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC CallLogService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Configuration Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
Dialing Rules Files	Good	OK	5/22/2018 7:49 AM	
NEC CTI Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Diag@Net Server	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC DirectoryService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Directory Synchronization Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC FrontEnd Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
Open Web Interface	Good	OK	5/22/2018 7:49 AM	
NEC License Manager	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC MessagingService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC PBXConfigurationService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC PresenceService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
Internal Presence	Good		5/22/2018 7:49 AM	
NEC RedundancyService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Remoting Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Reporting Service	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC SchedulerService	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC Social Media Proxy	Good	Service - Automatic / Started	5/22/2018 7:49 AM	
NEC UCC Proxy Service	Good	Service - Manual / Stopped	5/22/2018 7:49 AM	

Figure 11-2 System Health page

4. In case there are alarms, part of the window will be expanded to show alarm details, see figure below:



NEC RedundancyService	Good	Service - Automatic / Started	22/04/2013 12:42	
NEC Remote Call Control Service	Good	Service - Manual / Stopped	22/04/2013 12:42	
NEC Remoting Service	Good	Service - Automatic / Started	22/04/2013 12:42	
NEC Reporting Service	Good	Service - Automatic / Started	22/04/2013 12:42	
NEC SchedulerService	Good	Service - Automatic / Started	22/04/2013 12:42	
NEC UCC Proxy Service	Good	Service - Manual / Stopped	22/04/2013 12:42	
NEC VoiceMailService	Good	Service - Automatic / Started	22/04/2013 12:42	
NEC XML Push Service	Good	Service - Automatic / Started	22/04/2013 12:42	
SQL Server	Good		22/04/2013 12:42	Check
Server	Good	WIN-S9P97TL4ENQ, version: 10.50.1600	22/04/2013 12:42	
Status	Good	Status: Open , DB Size(MB): 120	22/04/2013 12:42	
Transaction Log	Good	Size(KB): 28000	22/04/2013 12:42	
Index fragmentation status	Good		22/04/2013 12:42	
Environment	Good		22/04/2013 12:41	Check
Disk Usage	Good		22/04/2013 12:41	
C:	Good	Total:29.20GB Free:8.56GB Used:71%	22/04/2013 12:41	
D:	Good	Total:119.66GB Free:55.75GB Used:54%	22/04/2013 12:41	
IP Connections	Good	Open: 1	22/04/2013 12:41	
IIS/W3SVC	Good	Status: Running	22/04/2013 12:41	
Secure Ports	Good	Binding: OK	22/04/2013 12:41	
Alarms	Failures		22/04/2013 12:42	Check
Active alarms	Failures	Number of alarms: 4. Hide	22/04/2013 12:42	

```
Current Active Alarms:
22/04/2013 12:40:52 [Monitoring Service]    85010002 NEC CallLogService is not running. Try to restart the service manually.
22/04/2013 12:40:04 [Monitoring Service]    84010001 UCS processes and/or service failure. View details in System Health page.
22/04/2013 12:39:11 [Monitoring Service]    85010003 NEC CTI Service is not running. Try to restart the service manually.
22/04/2013 12:37:00 [UCS Runtime Service] 84010001 UCS Runtime stopped.
```

System Info	Good		22/04/2013 12:38	Check

Figure 11-3 System Health page with alarms

11.2. BCT System Diagnostics

BCT is shipped with Diag@Net, an advanced diagnostic tool for problem detection. Using the Diag@Net, you can gather information about software problems or detect potential issues like configuration issues.

11.2.1. Understanding Diag@Net

Diag@Net supports two kinds of logging:

- Diagnostics, including application error reports and tracing
- System Status information

11.2.1.1. Diagnostics

There are five types of diagnostic messages:

Exception A significant problem, such as loss of functionality or loss of data. For example, if a service fails to start, an Exception message will be logged.

Warning A potential issue that might need user's attention. For example, when a user tried to login with incorrect credentials, a Warning message will be logged.

Event A message that describes the successful operation of an action. For example, when a service successfully synchronized with a PBX, an Information message will be logged.

Trace A message that reports the detailed flow of an application or service.

Status Information A message that denotes the current status of a (potential) issue. For example, when the system loses the connection to the PBX, an error status message will be logged. As soon as the connection has been restored, an error-reset status message will be logged. These messages will also be logged in the NEC System Status log, see below.

11.2.1.2. System Status

NEC System Status is a Windows Event log used by BCT application and services to report BCT system status.

This status information is also included in Diag@Net. In the System Status tab you can find an overview of open warnings and exceptions. When an abnormal situation occurs, an event will appear. As soon as the situation becomes normal again, the event will automatically disappear.

Note: *By default, System Status will only show events generated after the latest system restart.*

There are three types of status events:

Error A significant problem, such as connection loss or lack of disk space.

Warning An event that is not necessarily significant, but might need user's attention.

Information An event that either describes the successful operation of an action or reports a successful resolution for an error or warning reported earlier. For example, when the connection to a PBX has been restored an information event will be logged.

11.2.2. Using Diag@Net

By default the diagnostics service logs all exceptions and warnings.

The default location for the log files is in the following folder: "%SystemDrive%\NEC\Diagnostic Files". To change it, go to Tools > Options, File Administrator tab and specify another folder.

With the Diag@Net Monitor, you can see events as they happen and you can selectively choose which events to monitor.

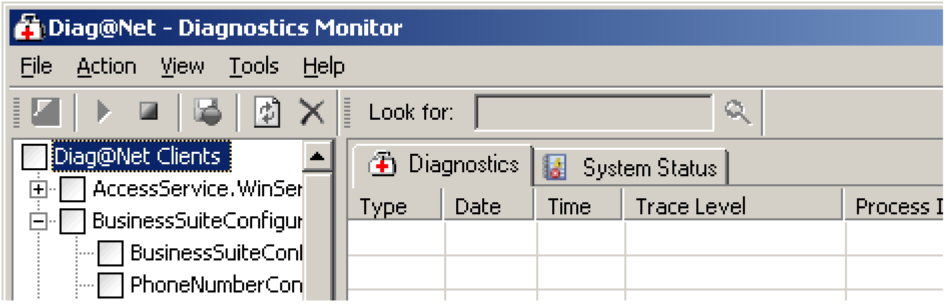


Figure 11-4 Diag@ Net Monitor

To launch the Diag@Net monitor:

1. Start/Programs/Business ConneCT/Tools/Diag@Net Monitor

To view diagnostic events:

1. Select the tab Diagnostics.
2. In the application tree you can then select which applications or services to actively monitor. Note that events (meaning successful operation of an action) and exception events are always written to the log file, regardless of the check state.

To enable detailed application tracing:

1. Go to Tools/Options/Trace Level.
2. Select the trace levels to log and monitor. Note that trace events are only written to the log file if the trace level is ticked.

To permanently delete all diagnostic log files:

1. Go to Tools > Options, File Administrator tab
2. Press Delete Files.

Templates

In BCT a couple of Diag@Net templates are included. A template is a predefined set of client and trace level settings. For example, to troubleshoot a call related issue, load the “Server – call and UCS behaviour.dtf” template, the appropriate trace levels will be ticked and logged.

By loading a template all current Application and Trace Level settings are reset.

To load a template file:

3. Go to “File/Load Template(s)”;
4. Select the template file and press Open.
5. To load multiple templates, hold down the Ctrl key, then click on the templates you want to load and then press Open.

Note: By default when loading a template all current settings will be reset. But this option can be unchecked in the Select templates dialog.

To create your own template file:

1. Select the application and/or trace level settings, then use "File/Save Template".

Recording

To record diagnostic events as they happen, click the **Record** button. Or, choose Action/Record Diagnostics Data from the menu.

To stop recording click the record button again.

Note: *if you don't stop recording, recording will continue until hard disk is full.*

11.2.3. BCT System Info Console

BCT is shipped with the System Info Console, a tool to gather all relevant information of the BCT server. The System Info Console output has to be added to a support request when a Service Engineer request support from the NEC Support desk.

The output can be generated in two ways:

- Via the graphical user interface
- Silent in the background, e.g. using a batch file which can be scheduled.

There are two ways to start the System Info Console:

1. On the BCT server, choose: "Start/Programs/Business ConneCT/Tools/System Info Console".

2. Via the System Health tray icon, "right mouse button" and select System Info Console.

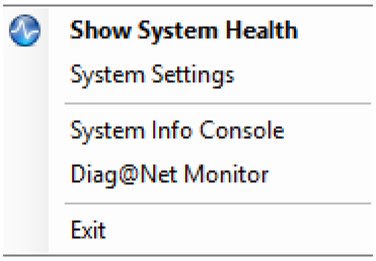
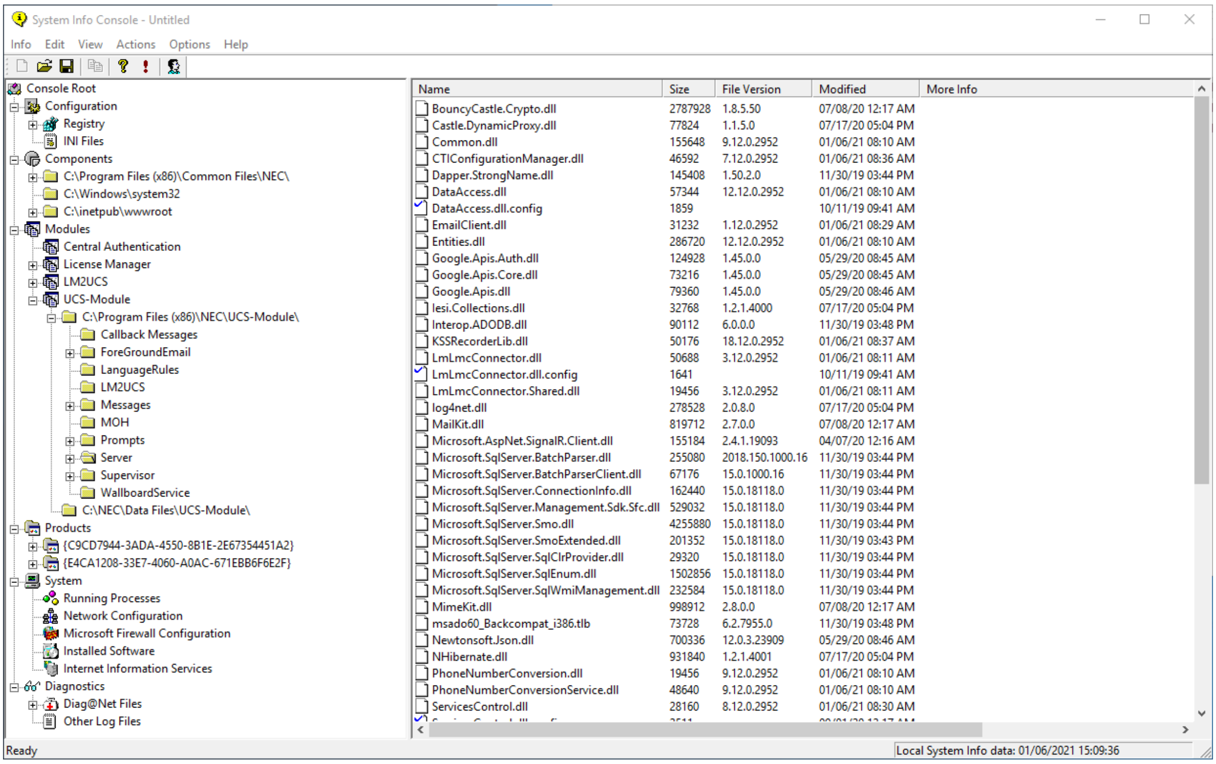


Figure 11-5 System Health taskbar icon and right mouse menu

The application is meant to collect product and system information into a so-called "snapshot". By default a full snapshot will be made (that can take a few minutes) but via menu "Options > Full Snapshot" one can disable the full snapshot mode and only core snapshot is made (not recommended).

To initiate (create) a snapshot select menu option "Info > Create new Snapshot". A progress bar is shown while the information is extracted.
When all information is retrieved, you can use "Options > Save As..." to save the data in a file.
The product/system meta data plus a number of product related files that were marked as attachment are all stored into a ZIP file. Via "Options > Attachments" it is possible to manage which file extenstions are included.

Below a typical example screenshot is shown after the full snapshot is made.


System Info Console - Untitled
Info Edit View Actions Options Help

```
Console Root
  Configuration
    Registry
    INI Files
  Components
    C:\Program Files (x86)\Common Files\NEC\
    C:\Windows\system32
    C:\inetpub\wwwroot
  Modules
    Central Authentication
    License Manager
    LM2UCS
    UCS-Module
      C:\Program Files (x86)\NEC\UCS-Module\
        Callback Messages
        ForeGroundEmail
        LanguageRules
        LM2UCS
        Messages
        MOH
        Prompts
        Server
        Supervisor
        WallboardService
      C:\NEC\Data Files\UCS-Module\
  Products
    {C9CD7944-3ADA-4550-8B1E-2E67354451A2}
    {E4CA1208-33E7-4060-A0AC-671EBB6F6E2F}
  System
    Running Processes
    Network Configuration
    Microsoft Firewall Configuration
    Installed Software
    Internet Information Services
  Diagnostics
    Diag@Net Files
    Other Log Files
```

Name	Size	File Version	Modified	More Info
BouncyCastle.Crypto.dll	2787928	1.8.5.50	07/08/20 12:17 AM	
Castle.DynamicProxy.dll	77824	1.1.5.0	07/17/20 05:04 PM	
Common.dll	155648	9.12.0.2952	01/06/21 08:10 AM	
CTIConfigurationManager.dll	46592	7.12.0.2952	01/06/21 08:36 AM	
Dapper.StrongName.dll	145408	1.50.2.0	11/30/19 03:44 PM	
DataAccess.dll	57344	12.12.0.2952	01/06/21 08:10 AM	
✓ DataAccess.dll.config	1859		10/11/19 09:41 AM	
EmailClient.dll	31232	1.12.0.2952	01/06/21 08:29 AM	
Entities.dll	286720	12.12.0.2952	01/06/21 08:10 AM	
Google.Apis.Auth.dll	124928	1.45.0.0	05/29/20 08:45 AM	
Google.Apis.Core.dll	73216	1.45.0.0	05/29/20 08:45 AM	
Google.Apis.dll	79360	1.45.0.0	05/29/20 08:46 AM	
Iesi.Collections.dll	32768	1.2.1.4000	07/17/20 05:04 PM	
Interop.ADODB.dll	90112	6.0.0.0	11/30/19 03:48 PM	
KSSRecorderLib.dll	50176	18.12.0.2952	01/06/21 08:37 AM	
LmLmcConnector.dll	50688	3.12.0.2952	01/06/21 08:11 AM	
✓ LmLmcConnector.dll.config	1641		10/11/19 09:41 AM	
LmLmcConnector.Shared.dll	19456	3.12.0.2952	01/06/21 08:11 AM	
log4net.dll	278528	2.0.8.0	07/17/20 05:04 PM	
MailKit.dll	819712	2.7.0.0	07/08/20 12:17 AM	
Microsoft.AspNet.SignalR.Client.dll	155184	2.4.1.19093	04/07/20 12:16 AM	
Microsoft.SqlServer.BatchParser.dll	255080	2018.150.1000.16	11/30/19 03:44 PM	
Microsoft.SqlServer.BatchParserClient.dll	67176	15.0.1000.16	11/30/19 03:44 PM	
Microsoft.SqlServer.ConnectionInfo.dll	162440	15.0.18118.0	11/30/19 03:44 PM	
Microsoft.SqlServer.Management.Sdk.Sfc.dll	529032	15.0.18118.0	11/30/19 03:44 PM	
Microsoft.SqlServer.Smo.dll	4255880	15.0.18118.0	11/30/19 03:44 PM	
Microsoft.SqlServer.SmoExtended.dll	201352	15.0.18118.0	11/30/19 03:43 PM	
Microsoft.SqlServer.SqlClrProvider.dll	29320	15.0.18118.0	11/30/19 03:44 PM	
Microsoft.SqlServer.SqlEnum.dll	1502856	15.0.18118.0	11/30/19 03:44 PM	
Microsoft.SqlServer.SqlWmiManagement.dll	232584	15.0.18118.0	11/30/19 03:44 PM	
MimeKit.dll	998912	2.8.0.0	07/08/20 12:17 AM	
msado60_Backcompat_i386.tlb	73728	6.2.7955.0	11/30/19 03:48 PM	
Newtonsoft.Json.dll	700336	12.0.3.23909	05/29/20 08:46 AM	
NHibernate.dll	931840	1.2.1.4001	07/17/20 05:04 PM	
PhoneNumberConversion.dll	19456	9.12.0.2952	01/06/21 08:10 AM	
PhoneNumberConversionService.dll	48640	9.12.0.2952	01/06/21 08:10 AM	
ServicesControl.dll	28160	8.12.0.2952	01/06/21 08:30 AM	

Ready

Local System Info data: 01/06/2021 15:09:36

Figure 11-6 System Info Console with System Info Data example

Next to the attachments included based on its extension one can also manually attach an additional file. Assume the service department wants to have a copy of Application prompt file 1002.wav. You would do the following:

1. Create the System Info Console information.
2. In the left pane, browse via Modules, UCS-Module to the prompt file.
3. In the right pane, select the file and open the “Actions > Attach” menu (or the Right Mouse Button).
4. Click on the “Attach” menu item to have file included when snapshot is saved.
5. Use Save to create the ZIP file. File 1002.wav will be added to the ZIP file.

System Info Console command line

It is possible to use the System Info Console from the DOS command line with options. The syntax is:

Option	Description
/s <Filename>	Save to file. Example: `SICONSOLE.EXE /s e:\temp\sic_01.sid`

/t abc — Items to add to “Infodata”.
Supported options:

- “r” - Information of the registry (Specific for BCT)
- “d” - Diag@Net files
- “c” - Information about the installed BCT components
- “m” - Information about the BCT modules used
- “s” – Information about the server

Typical example of the contents of a batch file could be:

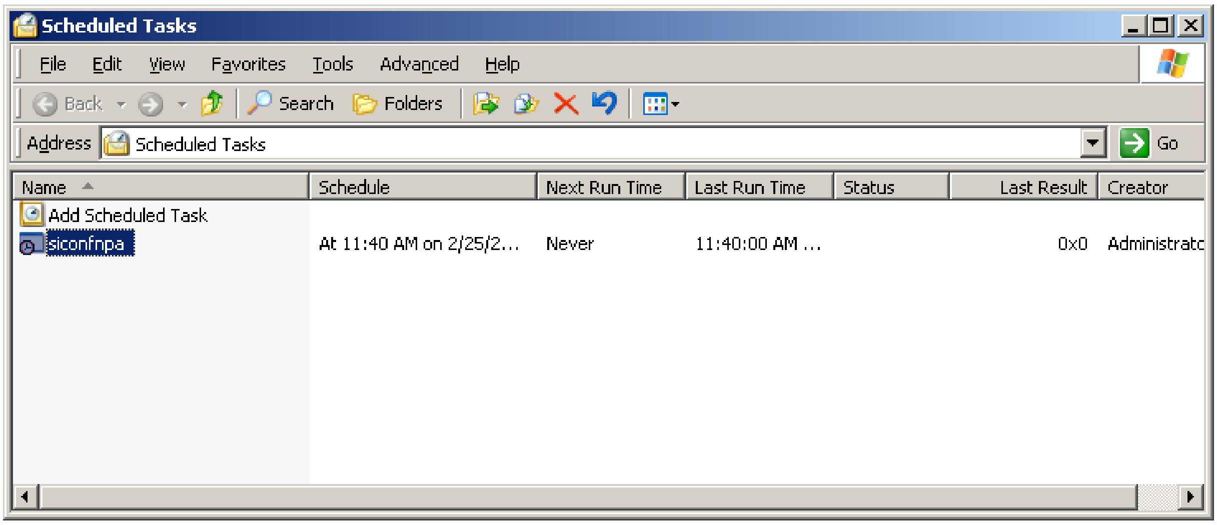
```
echo off
REM start System info console
REM change directory
c:
cd c:\
cd "C:\Program Files (x86)\Common Files\NEC\System Info Console"
REM execute and save information
siconsole /s c:\temp\system_info_console_01.sid /t rds
```

The windows scheduler can be used to generate periodical System Info Data. To add a task to the windows scheduler:

1. Go to Start/Control Panel and open Scheduled Tasks.

2. Move the cursor into the main window and click the right mouse button.

3. Select “New” and add a scheduled task. Next, enter a name for the task.



Name	Schedule	Next Run Time	Last Run Time	Status	Last Result	Creator
Add Scheduled Task						
siconfnpa	At 11:40 AM on 2/25/2...	Never	11:40:00 AM ...		0x0	Administratc

Figure 11-7 Scheduled Tasks window

4. Check the properties for the location and the user account settings, adjust the schedule and click apply (Use the correct credentials to run the application).

11.2.4. Using Windows Dump

NEC’s components may be adapted to provide more useful information in the rare case they are crashing. Currently this applies to:

- CTI Platform SDK (TSP component + CTI SDK DLL)

- Sopho CTI service

For this, the Windows Error Reporting (WER) functionality is used, which creates a so-called User-Mode dump at the moment a certain process is crashing. Such a dump contains the actual memory content and the process context at the moment of the crash. We can use this to follow the faulting executing flow.

Together with the NEC Diagnostics traces, WER gives much more support to NEC 4th line maintenance to track-down and isolate a possible bug.

The dump functionality is enabled by default and cannot be disabled. In case of a crash, automatically a dump will be generated in folder:

C:\NEC\MiniDumps [if using the default paths during installation]

Example of dump-file:

SophoCti.exe-20140625-163015.dmp
This indicates a dump of Sopho CTI Service that crashed 2014-06-25 at 16:30:15.

A maximum of 5 dumps will be stored for each process. After this, the oldest is deleted.

Note: *Windows Events will provide feedback on when crashes occurred.*

Note: *When a crash occurs in the TSP component (TAPI), the process names can be any of:* ***TapiSrv.exe****,* ***rundll32.exe*** *and* ***svchost.exe****.*

Note: *To prevent overwriting of tracing, always make a copy of the NEC Diagnostics traces immediately and provide these with the dumps when requesting support.*

11.3. Troubleshooting advice

11.3.1. Tracing

Problem: Help desk asked me for trace files to help problem solving, how and what should I trace...

Execute the following steps:

1. Use the Diag@Net tool, which is installed together with BCT on the server, to trace events in BCT. Start the Diag@Net monitor via: Start > Programs > Business ConneCT > Tools > Diag@Net Monitor (see 11.2 BCT System Diagnostics)

2. Use the System Info Console tool to generate a system overview report. Start the System Info Console via: start > Programs > Business ConneCT > Tools > System Info Console. The option “Create” generates a ZIP file and a SID file (system info data), the generated traces will be included in the ZIP file. Both files must be sent to help desk.

Always activate trace level settings for: UCS RAL (all), UCSCallHandler (all), BusinessOfficeServer (System, Call State, Call Events) and VMP Media Processing, [or load the “Server – call and UCS behaviour.dtf” template on the server].

Note: *There is also an extended version (“Server – Call and UCS behaviour – Comprehensive.dtf”), which traces for a longer period. But be aware that this will take up to 1 GB of hard disk space.*

For some of the most common items we suggest the following Trace Level settings:

Presence is not working correctly

Activate the Trace Level 'Business.OfficeServer - EagleEye Scanner' on the Server and 'Office Client Business Logic - Reachability' + 'Client – Login' on the Client.

Or, load the “Server – Reachability.dtf” template on the server + "Client – Login.dtf" template on the client.

Note: *For Presence related issues in a Univerge 3C environment, use the “Server – Presence and IM.dtf”*

Login failure on the Client

Activate all the Trace Levels of the 'Business.OfficeServer' on the Server and all Trace levels on the Client.

Or, load the “Client – Login.dtf" template on the client + "Server Login.dtf” template on the server.

Mismatch between extension and BCT client functionality

In Diag@Net monitor go to Tools/Options/Trace Levels, look for CTIServer and activate the following trace levels: 'Miscellaneous' / 'TSAPI Calls' / 'OAI Interfacing' / 'TSAPI Administration' and 'TSAPI CallId Administration' on the Server

Or, load the “Server – call and UCS behaviour.dtf” template on the server.

If the problem is not reproducible on short notice, you have to extend the size of the trace files. Go to Tools/Options/File Log Sizes, and change the size of the relevant log file. For example, for CTI Server select CTI Module/CTIServer and change Trace Log size to 50000 KB (This is already included in the template).

XML Application is not working correctly

Activate the tracing for XML application behavior by loading the “Server – XML Application.dtf” template on the server.

VMP Media Processing

Activate the tracing for VMP behavior by loading the "Server – VMP Media Processing.dtf" template on the server.

Multi-Line functionality

Activate the tracing for Multi-Line behavior by loading the "Server – Multi-Line.dtf" template on the server.

PBX Synchronization

Activate the tracing for PBX Synchronization behavior by loading the "Server – PBX Synchronization behaviour.dtf" template on the server.

Soft Wallboard

Activate the tracing for Soft Wallboard behavior by loading the “Client – SoftWallboard.dtf" template on the client + "Server - Softwallboard.dtf” template on the server.

Licensing / License verification

Activate the tracing for License verification behavior by loading the "Server - Licensing.dtf” template on the server.

Supervisor Dashboard

Activate the tracing of the Supervisor Dashboard behavior by loading the "Client - Supervisor Dashboard.dtf" template on the client and "Server - Supervisor Dashboard.dtf" on the Server.

Hotel / PMS Integration

Activate the tracing of the PMS hotel integration behavior by loading the "Server – PMS Connector.dtf" template on the Server.

Aranea / Data Synchronization

Activate the tracing of the Aranea data synchronization behavior by loading the "Server – Aranea.dtf" template on the Server.

After reproducing the error, make a copy of the 'C:\NEC\Diagnostic Files' directory on the Server and on the Client machine, when applicable. Add this information to the problem report.

If you encounter installation problems or the system is not ok after installation, please add the log file that was created during installation to the incident report. Include the setup log file named 'BusinessConneCT-Server_yyyymmddhhmmss' located in folder C:\Program Files (x86)\Common Files\NEC\Setup Log Files'.

Problem: How to make OAI (X.409) tracing...

When you are asked to provide OAI (X.409) tracing, you have to follow the next procedure:

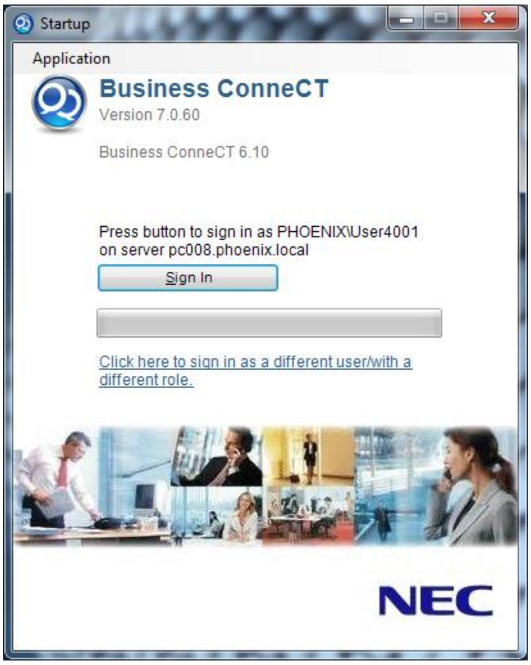
1. On the server machine goto the folder C:\NEC\Diagnostics Support\OAI Logging
2. Use the 'CTIService.OAILog.On.reg' file to activate the tracing, i.e. double click the file and accept execution;
3. Reproduce the problem, the OAI X.409 tracing is written in the file 'Local.LOG' in directory C:\WINDOWS\sysWOW64;
4. Use the 'CTIService.OAILog.Off.reg' file to de-activate the tracing, i.e. double click the file and accept execution;
5. Copy the Local.LOG file from C:\WINDOWS\sysWOW64 and attach it to the incident information.

Problem: A specific BCT client has problems. How can I get more diagnostic information for that client...

In the BCT startup screen on the client, press Ctrl+Shift and click on the NEC logo. You will be offered an Application menu.

Click on Application and select the option to Install Diagnostic tools, if you want to install Diag@Net. To start the monitor, click on C:\Program Files (x86)\Common files\NEC\Diag@Net\DiagMonitor.exe. See 11.2.2 Using Diag@Net.

Note: *See 12.1.1.3 Diagnostics in a Citrix environment in case your BCT Desktop Client runs in a Citrix or Terminal Services environment.*



Business ConneCT
Version 7.0.60

Business ConneCT 6.10

Press button to sign in as PHOENIX\User4001
on server pc008.phoenix.local

Click here to sign in as a different user/with a different role.

Figure 11-8 BCT startup screen with Application menu

11.3.2. Refresh behavior

Problem: New numbers, VMP lines or routing points are not visible in BCT...

After programming new numbers in the IS3000 / SV8100/SV9100 / AspireX/AspireUX / SV8300/SV9300 / SV8500/SV9500 these are not always automatically visible in BCT. The Synchronization process does not work in real-time.

To fix this, execute a ‘Reconnect to PBX Units’ using the BCT System Settings, see section 8.1.5 Connection to PBX. Mark the “Synchronize Once” or “Synchronize Always” check box. This will start a PBXSync process that will update the BCT database.

11.3.3. Server problems

Problem: When installing BCT server, a browser action towards the server fails

When installing BCT server (that is part of domain) a browser action towards the server might fail. An error page is shown with a text similar to "Page cannot be displayed" or "The requested URL could not be retrieved". Why?

In case the server is part of the domain, the server name used for configuration of BCT most probably is the FQDN. This means that also the URL is composed with that FQDN value, e.g. "http://PC065.UCSLAB.local/DirectoryBrowser/default.aspx". When a proxy server is used it will overrule the local DNS.

To properly have the URL resolved you should add the local BCT server to the proxy exception list. For the server computer this is typically being taken care of by the setup of BCT. However for client PCs that need to browse to BCT server (e.g. for install page of client application) the issue will occur as well. In this case, you have to add the exception manually:

1. Check 'Internet Options' > 'Connections' > 'LAN Settings' > 'Proxy Server - Advanced' if server is in exception list (e.g. PC065*) or ask your local system administrator to take care of this IT infrastructural issue.

Problem: How to change the server name

When having installed the BCT client related to a BCT server and having started the client application once the server name is fixed (field is disabled) – also applicable for user name and password – when you startup. How can I configure my client PC to use BCT client to be connected to another BCT server (or a server whose name has changed)?

The next step-by-step procedure should be used on the client PC:

1. Uninstall the BCT client package

2. Install BCTclient package (and use new server name – fill in when requested during UI sequence or pass as property value)

3. Start the BCT client package.
   Normally it should use the old server name when it is automatically started (and will fail).

4. From startup form press Ctrl + Alt and click on NEC logo. The Application menu + more information during login + change all fields options will appear.

5. Click the "Click here to login as a different user/with a different role" hyperlink. Now you will be able to change the server name.

6. Validate account and after this select **OK** to start the application

Problem: VMP is not working...

If your VMP lines are not working, first examine if the programming of the PBX is correct.

In case of an iS3000 / SV8100/SV9100 / AspireX/AspireUX / SV8300/SV9300 / SV8500/SV9500, if you register an IP DECT to one of the VMP line numbers it should be possible to make a call from any other extension to that VMP line, answer the call and have a both way speech path. If this is working, you can assume that the configuration is correct.

If changes are made to the network configuration of the computer on which you have installed the VMP software, check the NIC as used by VMP and, if necessary, change it. Tthis is described in section 8.1.1 Using the Configuration Wizard, step 11.

On systems that have multiple NICs with multiple IPs, it is possible that the default IP address picked by the VMP software may not be the IP address required for your situation. If this is also not the problem, collect the traces on the BCT Server and report an incident.

If the server has 2 or more network cards and VMP is of type "PROTIMS" then one possible reason the VMP lines are not working could be the wrong order of the network cards. The 'NEC DAP Controller (PDS) ' service requires a fixed order for the network interfaces: the network card that is part of the PBX network segment must be the first one on the list. The order can be changed by going to the Control panel, open Network Connections and choose Advanced Settings from the Advanced menu item.

11.3.4. Client problems

Problem: I receive any of the following login errors in the login screen

Note: *Per error number a possible solution is given.*

Error [01] - The extension is not being monitored
Stop/start of the UCSRuntime or there is a problem in the PBX with your extension number.
It may also mean that the extension was removed from the PBX and no PBX synchronization has been executed since then.

Error [02] - Internal error while claiming rights
NEC UCS Runtime Service is not started on the server. Start the service then try logging in again.

Error [03] - There are no more licenses available

There is no license available for this role

Error [04] - UCS reported agent not found
Restart NEC UCS Runtime Service. If it still fails, try to create the agent again.

Error [05] - UCS reported extension is already in use
Logout the user. Someone else is already using the extension.

Error [06] - The user name or password is incorrect
Mismatch in password – Redefine the password in BCT System Settings.

Error [07] - No connection possible to server
Cannot access the BCT server. Verify the network and verify that NEC Remoting Service is started on the server.

Error [08] - Communication with call service (UCS) failed

Can't access NEC UCS Runtime Service. Start or restart the service, then try again.

Error [09] – Invalid Extension number
You're trying to use a free seating extension which is not valid any more.

Error [10] – Invalid User role
Contact your system administrator; your role might have been removed while user was logged in.

Problem: A security warning appears when a BCT application is started...

Such a warning might popup when the application is started for the first time, for instance the Web directory. Click Install and accept content from NEC Nederland B.V.

Problem: I cannot restore the BCT client window, although it is still visible on the taskbar...

Most likely the 'DesktopClient.xml' file became corrupt. This may happen when you force a shutdown of the PC while the BCT client window is still closing.

To solve this, delete the 'DesktopClient.xml' file or change some settings in the file. When you delete this file, you have to enter the BCT Server information after you start the client again. When you edit this file, this is not necessary.

You'll find the file on the BCT client PC on the following location:
"C:\Users\<account>\AppData\Roaming\NEC\DesktopClient"

Note: *The pathname may be Operating System dependent. Search on 'DesktopClient.xml' if you can't find it immediately.*

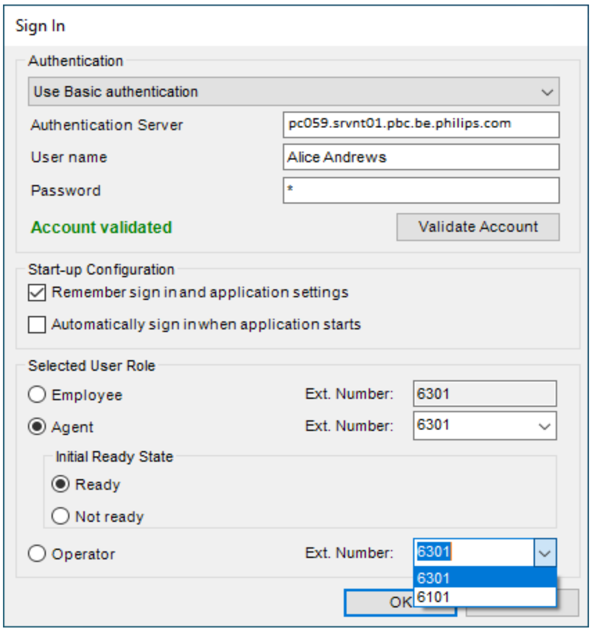
Problem: Not able to login with Windows Authentication...

Reason for this problem could be that the BCT client does not send enough information to the BCT server to be able to identify the user and login. The login process stops with the error message is 'UCS reported: Agent Not Found'.

To bypass this problem change the parameter 'isLoginBoxInfoLimited' value from 'true' to 'false'. This parameter is in the file “RemotingService.WinService.exe.config” in the folder C:\Program Files (x86)\Common Files\NEC\Services on the BCT server.

Problem: How to modify the login name and password...

After a successful logon the user is not able to modify the settings. The authentication fields are disabled, see Figure 11-9 Login window.



Sign In

Authentication

Use Basic authentication

Authentication Server: pc059.srvnt01.pbc.be.philips.com

User name: Alice Andrews

Password: *

Account validated

Start-up Configuration

☑ Remember sign in and application settings

☐ Automatically sign in when application starts

Selected User Role

○ Employee — Ext. Number: 6301

● Agent — Ext. Number: 6301

Initial Ready State

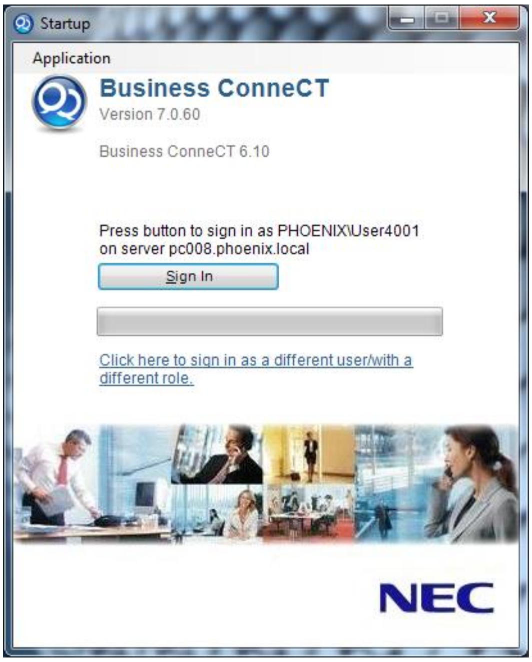
● Ready

○ Not ready

○ Operator — Ext. Number: 6301

Figure 11-9 Login window

It is however possible for an engineer to enable the servername field again. Hold down the left Ctrl+Alt key and click on the NEC logo in the startup window. Now the “Application” menu appears. See Figure 11-10 Startup window with Application menu.



Startup

Application

Business ConneCT

Version 7.0.60

Business ConneCT 6.10

Press button to sign in as PHOENIX\User4001 on server pc008.phoenix.local

Sign In
Click here to sign in as a different user/with a different role.
NEC

Figure 11-10 Startup window with Application menu

Now the Servername field is enabled again. If you want to change the username, exit the login, and start login again.

Note: *Don't forget the disable the Application menu. Hold the Ctrl key and click on the NEC logo to disable the Application menu.*

Problem: Sometimes the BCT window does not pop-up on an incoming call...

This is because other applications use similar functionality to get or stay on the foreground. We cannot prevent that another application overrules the pop-up of our BCT client.

Problem: Another operator cannot start BCT...

If an operator does not log off properly or the pc crashes or the LAN connection is gone, then the BCT license is not released properly. Now if another operator tries to log into BCT, there is a time-out (8 to 15 minutes) you have to wait for, before the license is released.

Problem: Client cannot play voicemail messages via the phone...

If the server PC has multiple network interfaces and clients experience problems with voicemail, execute the steps described in section 11.3.3 Server problems, listed under the problem "System does not start up".

Problem: The sound quality is poor...

If all calls have poor sound quality, there may be problems with the codec settings. The settings of the VMP lines must match with the PBX.

It is recommended for VMP lines to use codec G.711 a-Law (outside the EU µ-law instead of A-law can be used). Check the PBX codec settings and the codec settings in BCT Supervisor Dashboard > Tools > Configuration > Media ports.

Problem: Answer icon is not enabled when I receive a call...

When the answer-icon is not enabled when you receive a call, check the terminal type of the extension. See 8.5.1 Extension Configuration (Company Directory).

Problem: I have another problem...

Check if the computer's network card is not used or no cable is connected. If so, disable the not-used network card.

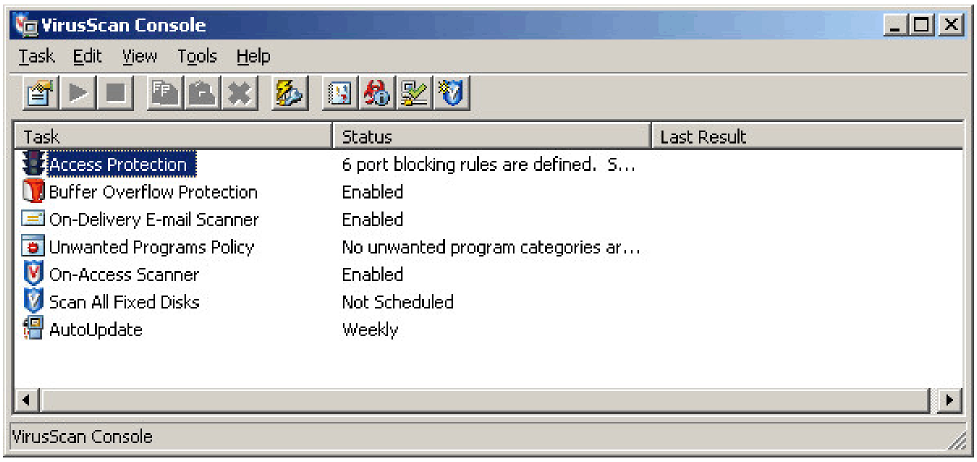
Check if the client and the server are in the same time zone. Synchronize the time.

11.3.5. Email problems

11.3.5.1. McAfee blocks email port

If you encounter a problem using email integration, you may need to tell McAfee that BCT is a 'trusted' program for sending emails. Perform the following steps:

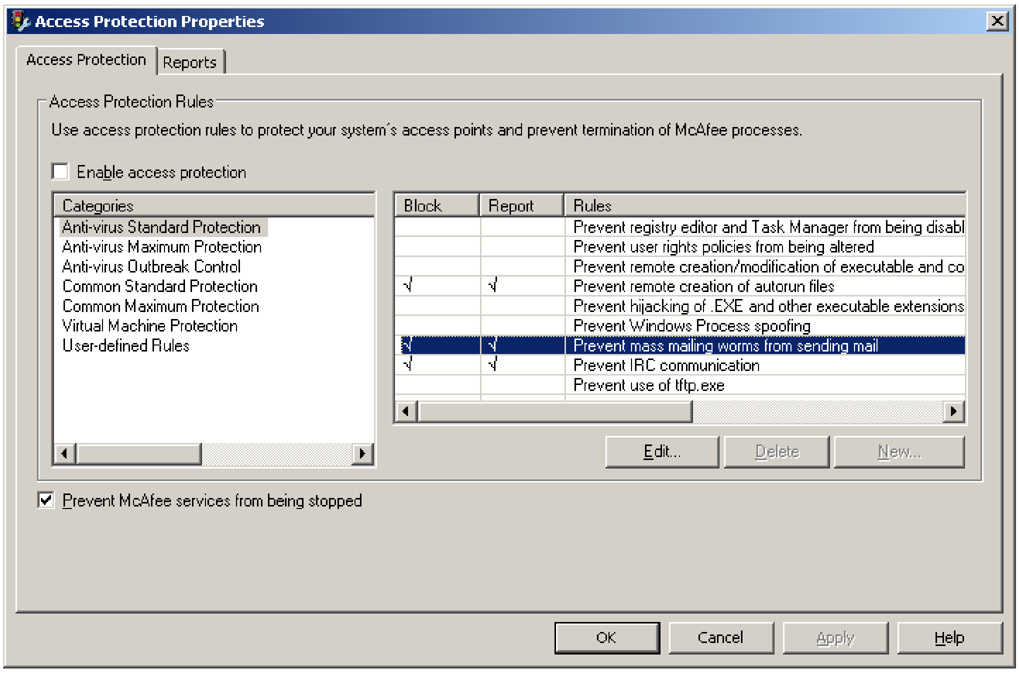
1. Open the VirusScan console.



Task	Status	Last Result
Access Protection	6 port blocking rules are defined. S...	
Buffer Overflow Protection	Enabled	
On-Delivery E-mail Scanner	Enabled	
Unwanted Programs Policy	No unwanted program categories ar...	
On-Access Scanner	Enabled	
Scan All Fixed Disks	Not Scheduled	
AutoUpdate	Weekly	

Figure 11-11 McAfee VirusScan Console

2. Double click the 'Access Protection' task.



Access Protection Rules

Use access protection rules to protect your system's access points and prevent termination of McAfee processes.

☐ Enable access protection

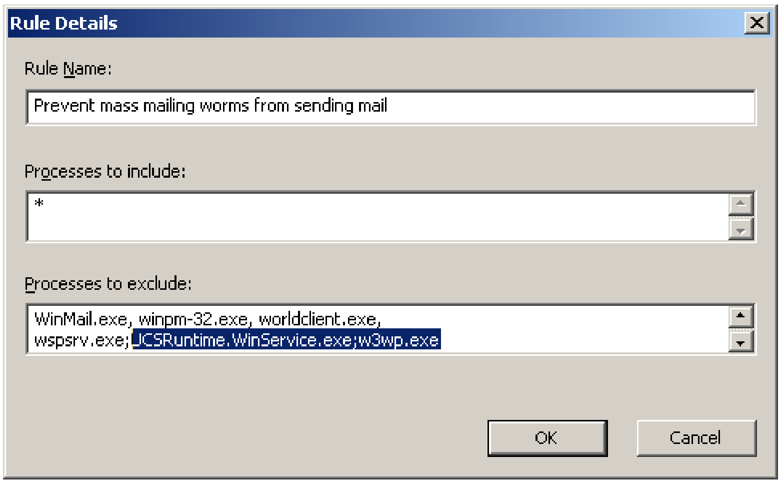
Categories
Anti-virus Standard Protection
Anti-virus Maximum Protection
Anti-virus Outbreak Control
Common Standard Protection
Common Maximum Protection
Virtual Machine Protection
User-defined Rules

Block	Report	Rules
		Prevent registry editor and Task Manager from being disabl
		Prevent user rights policies from being altered
		Prevent remote creation/modification of executable and co
√	√	Prevent remote creation of autorun files
		Prevent hijacking of .EXE and other executable extensions
		Prevent Windows Process spoofing
√	√	Prevent mass mailing worms from sending mail
√	√	Prevent IRC communication
		Prevent use of tftp.exe

☑ Prevent McAfee services from being stopped

Figure 11-12 McAfee Port Blocking

3. In the Ports to Block section, select the **Prevent mass mailing worms from sending mail** and click **Edit**.



Rule Name:

Prevent mass mailing worms from sending mail

Processes to include:

*

Processes to exclude:

WinMail.exe, winpm-32.exe, worldclient.exe,
wspsrv.exe;UCSRuntime.WinService.exe;w3wp.exe

Figure 11-13 McAfee Edit rule

4. In the Processes to exclude box, add UCSRuntime.WinService.exe and w3wp.exe.

11.3.6. VMP lines

Problem: BCT Supervisor doesn’t show the VMP lines (Media ports)

When after an upgrade of BCT, the VMP lines are not visible in the Configuration screen of the BCT Supervisor Dashboard, check the properties of the VMP lines and IVR group in the PBX against the information in this manual.

11.3.7. Fallback

Problem: UCS stopped but fallback scenario is not activated...

The Fallback in the PBX is activated by the Day/Night status of the Routing Points. When a monitor is active, the status is day, otherwise it is night.

To enter the Fallback mode: stop the UCS RunTime monitoring service.

11.3.8. Database

Problem: How can I connect to the BCT database

If you need to manually establish an ODBC database link to an SQL database, or select another database for testing purposes, and use known SQL login credentials:

- User name: sa
- Password: [sa-password]

Problem: Move database to different SQL server

When you want to change your BCT configuration to use a different SQL server, changes on both the BCT server and the BCT Supervisor Dashboard clients are necessary. Since this is not a commonly supported action, it is not described in the manual. For more information please refer to the BCT FAQ ‘BCT 4.5.2 and up: How to move the DB to a new SQL server?’ and/or contact the Support Center.

11.3.9. Central Authentication

Problem: Central Authentication is not working anymore after installation of Aranea...

Aranea installs new services/accounts on the Server. These services/accounts do not have the same password as the other services/accounts. For this reason these services/accounts cannot interact.

To solve this: synchronize the passwords of all services via the Security Configurator (part of support tools, which is installed together with BCT), i.e. start Security Configurator, select tab 'Identity', select modify, select 'Renew', select 'OK', select 'Apply' and 'OK'. Reboot the BCT Server.

11.3.10. Contact Center problems

Problem: General Supervisor account does not get emails if routing fails...

Reason for this problem could be that one of the agents has an email address that is not valid. In this case, when incoming email is routed to the miss-configured agent, the email server will send back the email to the sender, which is the email address of the Contact Center.

In systems where this problem occurs due to unknown reasons, the system administrator should create an email rule with keywords (body or subject) from the rejected-warning from the email server. Now these failure announcements will follow a specific path, defined by the rule made for it.

11.3.11. Operator Fallback indication does not work

When a call arrives for the second time by the operator it will appear in the Fallback Queue with an indication. ↳

This indication is controlled a timer in the PABX and a timer in BCT. The time defined in BCT (default 38 seconds) has to be larger than the time in the PABX. If the time in BCT is smaller each call in the fallback Queue will appear without an indication.

To change this timer in BCT:

1. Create the '"RecallTimeForTransferredCalls" registry key on the server as follows: [HKEY_LOCAL_MACHINE\SOFTWARE\Philips\UCS\CtiCsta\RecallTimeForTransferredCalls] (32 bit OS) or[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Philips\UCS\CtiCsta\ RecallTimeForTransferredCalls] (64 bit OS).

   Add the value as a DWORD. The default value is 38 seconds.
   When set to 0, no fallback information will be given.

2. Restart the BCT via the Runtime Manager to activate the change.

11.3.12. Cannot configure Location Diversity when editing PBX settings

It may occur after a new installation of BCT on a SV8500/SV9500 Location Diversity or SV9500-Geo system, that the option "Support Location Diversity" is not present in the GUI. Should that be the case then restart the NEC Redundancy service from the services applet and refresh the system settings connectivity tab page.

11.3.13. Call Forwarding No Answer to Voicemail

If you have Number Conversion between a DDI number range (called from outside) to an internal number range, and you call an extension in that range, that has Call Forwarding set to Voicemail, then please take note of the following:

For all PBX-types, except iS3000 and UNIVERGE 3C:

- In case the Call Forwarding is applied directly (e.g. Call Forwarding – All) this works fine, the call is forwarded correctly, based on the converted number.

- In case the Call Forwarding is delayed (e.g. Call Forwarding – Don't Answer) then the converted number is not used, and the call is not forwarded correctly. However, it can be configured to use the converted number for delayed forwarding to voicemail, by setting registry key:

  32 bit OS: [HKEY_LOCAL_MACHINE\Software\Philips\STSAPI Module\OAI]
  Define string 'IgnoreDDINumber' with value "True".
  64 bit OS: [HKEY_LOCAL_MACHINE\Software\Wow6432Node\Philips\STSAPI Module\OAI]
  Define string 'IgnoreDDINumber' with value "True".

11.3.14. Agent Display Information overwritten

In some cases (for instance in Hotel mode) it may be the case that an external integrated system writes information to the agent terminal display. However, BCT may also send information to the agent terminal display, such as the called number, DNR of the caller and the router name, overwriting the previous information.

To suppress BCT writing call information to the agent terminal display:

1. Open the file UCSRunTime.WinService.exe.config, with the Notepad editor for example. Most likely location: C:\Program Files (x86)\NEC\UCS-Module\Server.

2. Enable / include:

```
<add key="SendDisplayTextToTerminal" value="false"/>
```

11.3.15. How to disable "away" status

In some situations the "away" indication of the BCT Desktop Client must be disabled, because the user may have several PC's, so it is not visible when the user is available.

To disable the "away"-feature system-wide, execute the following steps:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config”.

2. Locate the key: AwayTime

3. Change the default value (15) by 0 if you want no away timing.

4. Press button Save to store the value.

5. Restart the Remoting Service (or the whole system)

11.3.16. Social Media Attachment problems

If the Desktop Client cannot open an attached file in a social media chat session, it may be that the file extension is blocked by the IIS of the BCT Server.

On the BCT Server open the IIS Manager and select folder “Sites\Default Web Site\SocialMediaAttachments”. Open the “MIME Types” settings and check if the extension of the attached file is in the list.

If the extension of the attachment is not in the list, add the extension and the associated MIME Type.

11.3.17. Social Media Proxy service logging

Like other BCT services, the NEC Social Media Proxy service can log to the Diag@Net application and you will find “SocialMediaProxy.exe” in the list of Diag@Net Clients.

While for other BCT services the log levels are configured in the Diag@Net Diagnostics Monitor application, the trace levels of the NEC Social Media Proxy service are configured in the configuration file of the service.

In Diag@Net, the log messages of the Social Media Proxy service will all be shown as information messages.

Like for other BCT services, the messages are written to a diagnostics file, but only to the EventException.txt file, typically in the folder “C:\NEC\Diagnostic Files\SocialMediaProxy\’ on the BCT server. The maximum file size and the number of files can be configured via the Diag@Net Diagnostics Monitor application (Options – File Log Size).

To change the log levels of the Social Media Proxy service:

1. On the BCT server, browse to "C:\Program Files (x86)\Common Files\NEC\ Social Media Proxy " and use a text editor (e.g. Notepad) to open the file “appsettings.json” and locate the "Logging" section:

```
{
  …,
  "Logging”: {
    "IncludeScopes": false,
    "Debug": {
      "LogLevel": {
        "Default": "Warning"
      }
    },
    "Console": {
      "LogLevel": {
        "Default": "Warning"
      }
    },
    "ApiProxyLog": {
      "LogLevel": {
        "Default": "Warning"
      }
    },
    "LogLevel": {
      "Default": "Trace"
    }
  },
  …
```

2. To maximize log information, change the "Warning" levels into "Trace". Other levels are "Critical", "Debug", "Error", "Information" and "None".

3. Save and close the file

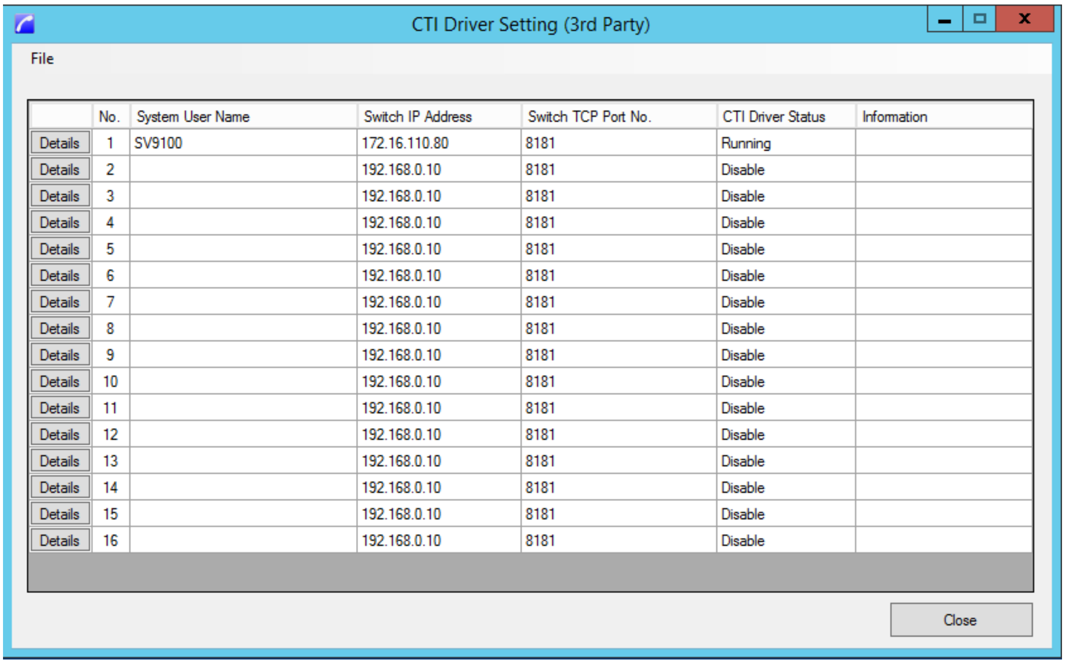
4. Restart the service NEC Social Media Proxy or the Business ConneCT computer.

11.3.18. SV9100 TAPI Connection problems

For SV9100-TAPI environments BCT does not connect directly to the PBX CTI interface but uses extra driver software that is installed on the BCT system. This driver needs to have a correct status to allow BCT to connect properly to the PBX. If the driver is not functioning correctly, BCT will not be able to establish the CTI connection and no voice calls can be routed nor controlled.

This driver can be managed using the “CTI Driver Configuration Tool” that can be found on the BCT server in the Start Menu under “NEC”.

When opening the next screen is shown:

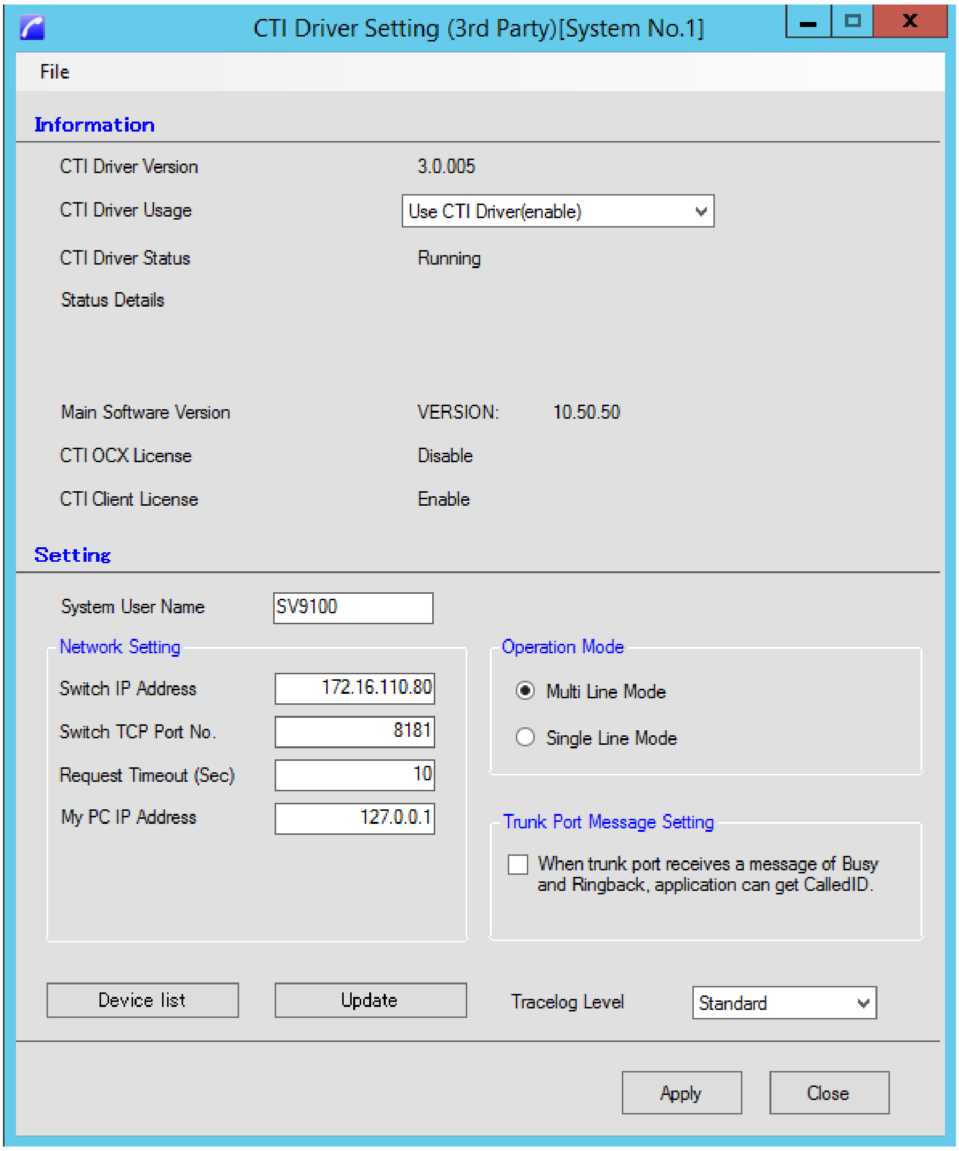


	No.	System User Name	Switch IP Address	Switch TCP Port No.	CTI Driver Status	Information
Details	1	SV9100	172.16.110.80	8181	Running	
Details	2		192.168.0.10	8181	Disable	
Details	3		192.168.0.10	8181	Disable	
Details	4		192.168.0.10	8181	Disable	
Details	5		192.168.0.10	8181	Disable	
Details	6		192.168.0.10	8181	Disable	
Details	7		192.168.0.10	8181	Disable	
Details	8		192.168.0.10	8181	Disable	
Details	9		192.168.0.10	8181	Disable	
Details	10		192.168.0.10	8181	Disable	
Details	11		192.168.0.10	8181	Disable	
Details	12		192.168.0.10	8181	Disable	
Details	13		192.168.0.10	8181	Disable	
Details	14		192.168.0.10	8181	Disable	
Details	15		192.168.0.10	8181	Disable	
Details	16		192.168.0.10	8181	Disable	

Figure 11-14 CTI Driver Configuration Tool overview

In a BCT system with one SV9100-TAPI PBX configured, only the first line will be configured. When more than one SV9100-TAPI PBX is configured, each PBX has its own line in this overview.

Press “Details” for the relevant PBX and the next screen is shown:



Information

CTI Driver Version 3.0.005

CTI Driver Usage Use CTI Driver(enable)

CTI Driver Status Running

Status Details

Main Software Version VERSION: 10.50.50

CTI OCX License Disable

CTI Client License Enable

Setting

System User Name SV9100

Network Setting

Switch IP Address 172.16.110.80

Switch TCP Port No. 8181

Request Timeout (Sec) 10

My PC IP Address 127.0.0.1

Operation Mode

● Multi Line Mode

○ Single Line Mode

Trunk Port Message Setting

□ When trunk port receives a message of Busy and Ringback, application can get CalledID.

Tracelog Level Standard

Figure 11-15 CTI Driver Configuration Tool details

Here the actual configuration and status of the Driver for this PBX is shown and can be managed. The next items are the most relevant:

- **CTI Driver Usage**:
  With this dropdown the driver status can be managed:
  - Use CTI (enable)
    The driver is requested to connect to the PBX
  - Not use CTI (disable)
    The driver is requested to disconnect from the PBX
- **CTI Driver Status**
  - Running
    ➔ “CTI Driver Usage” = Use CTI (enable)
    The Driver has established connection with the PBX, BCT **can** establish CTI connection with the PBX

    - Disable
      ➔ “CTI Driver Usage” = Not use CTI (disable)
      The Driver has stopped connection to the PBX, BCT **cannot** establish a CTI connection to the PBX
    - Connection Error
      ➔ “CTI Driver Usage” = Use CTI (enable)
      The Driver experiences (IP) connection problems between the BCT server and the PBX, BCT **cannot** establish a CTI connection to the PBX
    - Any other status
      The Driver is trying to restore the connection or make a transition to the requested state in the CTI Driver Usage dropdown, BCT **cannot** establish a CTI connection to the PBX
- **Main Software Version**
  The software version of the SV9100
- **CTI Client License**
  Enable: TAPI usage is licensed in the PBX (i.e. License code 0112 is available)
- **Tracelog Level**
  Dropdown were the degree of logging can be managed, “Detail” should be selected only when there are severe problems to be analysed by NEC. Press “Apply” to activate the change.
  The logging output can be found in folder “C:\Program Files\NEC\CTIDriver(3rd)\Log\SysXX” where XX indicates the system number from the overview (typically XX=01).
- **Button “Apply”**
  When “CTI Driver Usage” dropdown value has been changed, press this button to activate the selection. A popup will be shown to verify the selection, press OK to continue otherwise press Cancel. After some time a new popup will be shown when the requested transition has been executed, press OK.
- **Button “Close”**
  To leave the details, press this button. The overview wil be shown, press the Close button to leave the “CTI Driver Configuration Tool”.

When CTI Driver Status not indicate “Running”, try to disable the driver and re-enable it again. When that does not help, check the (IP) connection path between BCT server and PBX. A reboot of the BCT server PC might also help.

11.3.19. Secure Port Binding problems

When in the health page it is indicated that there are secure port binding errors (i.e. the “Secure Ports” line does indicates failures), Use the *Server Manager* application to repair the port binding errors.

11.4. BCT Alarms

11.4.1. What is a BCT Alarm

A BCT Alarm is a message from BCT that an error situation has occurred somewhere in the BCT system. The Alarm is meant for the (1st or 2nd) line service engineer, who has to take some kind of action. The required action is indicated by the Alarm.

Alarms are presented to the service engineer:

1. in the System Settings Health page (See Figure 11-2 System Health page).
   The Health page shows only the Alarms that are currently active (SET but not yet RESET).

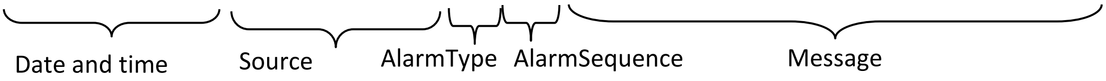
2. in the Diag@Net Event Log (See 11.2.1 Understanding Diag@Net).
   Use the Event Viewer, NEC System Status event log.
   This log contains actual and historic information: all Alarm SET and RESET events are shown.

Alarms are set and reset by the BCT system. A SET is given when the error situation is detected, a RESET is given when the error situation is resolved.

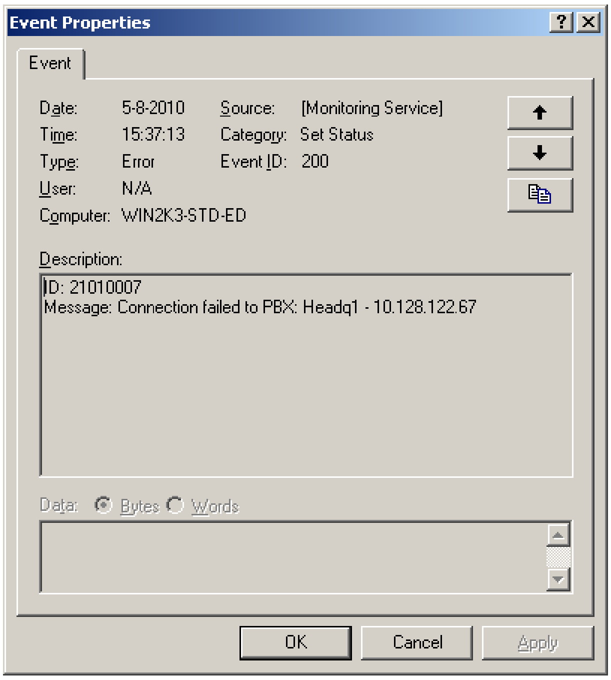
11.4.2. Presentation of a BCT Alarm

In the **System Health page**, an Alarm looks like:

8/5/2010 3:37:13 PM [Monitoring Service] 21010007 Connection failed to PBX: Headq1 - 10.128.122.67



In the **NEC System Status** event log an Alarm looks like:



Date: 5-8-2010
Time: 15:37:13
Type: Error
User: N/A
Computer: WIN2K3-STD-ED
Source: [Monitoring Service]
Category: Set Status
Event ID: 200

Description:

ID: 21010007
Message: Connection failed to PBX: Headq1 - 10.128.122.67

Data: ● Bytes ○ Words

Figure 11-16 NEC System Status BCT Alarm layout

In both presentations, the parameters are the same:

Date and Time	The date and time the alarm was raised. When an error situation remains for some time, only the first time the error was detected an Alarm is raised.
Source	The process that raised the Alarm.
Alarm Type	The first 4 digits of the alarm ID indicate the type of error that caused the Alarm. Alarm Types relate to the sections of chapter 11.4.3 List of BCT Alarms. In these sections you can find the required actions to solve (or report) the error.
Alarm Sequence	The last 4 digits of the alarm ID indicate an internal sequence number (not relevant for the system engineer).
Message	A short explanation of the error causing the alarm, with possible details like a PBX name, an IP address, etc., to give the service engineer additional information to solve the problem. The messages that can be given for each Alarm are listed in chapter 11.4.3 List of BCT Alarms.

11.4.3. List of BCT Alarms

The following sections list the BCT Alarms.

11.4.3.1. Network connection lost Alarm [1101]

Alarm Type	1101
Description	General Server Alarm - Network connection lost
Severity	Error
Explanation	The BCT Server has no connection to the network anymore for some time.
Additional Info	-
Required actions	• Check the physical connection of the BCT server to the network. Re-insert the removed connectors, if any. • Check the Connection status at Windows 'Network Connections'. Take any actions required to establish the connection. After the connection has been established again the system will recover automatically.

11.4.3.2. PMS connection lost [1102]

Alarm Type	1102
Description	PMS connection lost
Severity	Error
Explanation	The PMS controller has no connection to the PMS system anymore for some time.
Additional info	-
Required actions	• Check if PMS system is up and running. • Check the physical connection of the server to the network. Replace removed connectors, if any. • Check the Connection status at Windows 'Network Connections'. Take any actions required to establish the connection. After the connection has been established again the system will recover automatically.

11.4.3.3. Disk usage Alarm [1201]

Alarm Type	1201
Description	General Server Alarm - Disk usage problem
Severity	Error
Explanation	One or more of the fixed hard disks on the system is used for more than 95%.
Additional Info	Disk drive identity
Required actions	• Check the size of the database translation log and shrink the transaction log if required. • Delete any old and unnecessary log files, like IIS log files. • Delete any other unused files. • Adapt distribution of files over the hard disks. When the disk usage has been adapted no further actions are required.

11.4.3.4. Virtual Memory usage Alarm [1202]

Alarm Type	1202
Description	General Server Alarm - Virtual Memory usage problem
Severity	Error
Explanation	The system uses more than 98% of virtual memory for longer than 5 minutes. A memory leak might be threatening the system.
Additional Info	-
Required actions	• Check virtual memory usage with the Windows Task Manager. Restart any application with excessive virtual memory usage.

11.4.3.5. Windows Service not running Alarm [1401]

Alarm Type	1401
Description	General Server Alarm - Windows Service not running
Severity	Error
Explanation	A general Windows Service that is used by BCT is not running.
Additional Info	Name of the service
Required actions	• Restart the Windows Service manually. After the service has been restarted no further actions are required.

11.4.3.6. PBX connection Alarm [2101]

Alarm Type	2101
Description	PBX Alarm - PBX connection problem
Severity	Error
Explanation	An error occurred during connection to the PBX.
Additional Info	PBX identification
Required actions	• Check if the BCT server is still connected to the network. If not, you will probably have more Alarms about connections. Re-establish the connection to the network. The PBX connection will recover automatically. • Check the configuration in System Settings – Connectivity. If the IP-address or Port of the PBX is incorrect, correct the settings. • Check if the IP connection to the PBX is correct (PING). If you can reach the network but the PING fails, check the status of the PBX and possibly other components like routers, bridges etc. When the connection has been re-established the PBX connection will recover automatically.

	• Check that the required licenses on the PBX are present. If not, change the PBX licenses. The PBX connection will recover automatically. • If the failing connection is the CTI connection (see the source field in the message), please restart the NEC CTI Service. iS3000 only: • Check that the unit number of the PBX is the same as specified in the System Settings page (iS3000). If the unit number is incorrect, synchronize the PBX. Check that the PVE Service is started on the PBX (with PBX command 'DISRVC:0'). If the service is not started, start with 'STSRVC:0'. The PBX connection will recover automatically. SV9100-TAPI only: • Additional info also contains information about the CTI Driver status • For more additional actions see section *11.3.18 SV9100 TAPI Connection problems*

11.4.3.7. PBX Command timeout Alarm (UNIVERGE 3C only) [2102]

Alarm Type	2102
Description	PBX Alarm - PBX command timeout problem
Severity	Error
Explanation	An error occurred during command execution to the PBX.
Additional Info	PBX identification
Required actions	UNIVERGE 3C only: • PBX[IP.address] cmd timeout for DNR[endpoint] The 3C command execution response for the endpoint took more than 6 seconds. Check the endpoint and actions of 3C during this time. • After 100 successful commands the error is reset.

11.4.3.8. PBX connection Alarm [2103]

Alarm Type	2103
Description	PBX Alarm - PBX connection authorization problem
Severity	Error
Explanation	An error occurred during login to the PBX.
Additional Info	PBX identification, user name
Required actions	• Check the configuration in System Settings – Connectivity. If the username and password of the PBX is incorrect, correct the settings. • Check if the PBX user has sufficient rights.

11.4.3.9. VMP connection with SIP server (PBX) Alarm [2110]

Alarm Type	2110
Description	PBX Alarm - VMP connection problem with SIP Server (PBX)
Severity	Error
Explanation	VMP Service cannot contact SIP Server (PBX) to register its SIP IVR-lines.
Additional Info	PBX name, SIP VoIP Server (PBX) IP address + port
Required actions	• Check if the server (where VMP Service is running) is still connected to the network. If this is not the case, and VMP Service is running on the BCT Server, you will probably have more connection Alarms.

	Action: Re-establish the connection to the network. The PBX connection will recover automatically. • Check the connectivity configuration. If the IP-address and/or Port of the SIP Server (PBX) are incorrect, change the settings and restart BCT. • Check if the IP connection to the PBX is correct (PING). If you can reach the network but the PING fails, check the status of the PBX and possibly other components like routers, bridges etc. When solved, the PBX connection will recover automatically. • Check if the SIP Service is available/running on PBX (license, settings, …). If not, correct this and check if BCT also requires re-sync. If required restart the PBX and BCT. • Check if there are enough lines projected. • Check if a line could not be registered due to wrong username/password. After the adaptations the system will recover automatically.

11.4.3.10. Location Diversity Network Error [2120]

Alarm Type	2120
Description	PBX Alarm – Connection problem
Severity	Error
Explanation	The master node of a location diversity node is not available or there are problems in the location diversity network.
Additional Info	PBX name, IP address
Required actions	• Check that the BCT server is still connected to the network. • If you can reach the network but the PING fails, check the status of the PBX and possibly other components like routers, bridges etc. When solved, the location diversity network will recover automatically.

11.4.3.11. Location Diversity Node Error [2121]

Alarm Type	2121
Description	PBX Alarm – Problem in Location Diversity Node
Severity	Error
Explanation	The node in a location diversity node is not available or there are problems in the location diversity network.
Additional Info	PBX name, IP address
Required actions	• Check that the BCT server is still connected to the network. • If you can reach the network but the PING fails, check the status of the PBX node and possibly other components like routers, bridges etc. When solved, the connection to the node will recover automatically.

11.4.3.12. Automatic Failover[2130]

Alarm Type	2130
Description	Automatic failover executing to alternative node in PBX redundancy network.
Severity	Error
Explanation	Automatic failover executing to alternative node in PBX redundancy network, because the connected node was not available anymore.
Additional Info	PBX identification, Failover destination, Failover reason.
Required actions	• Check the status of the PBX nodes on the PBX and take proper actions to make the preferred PBX node active again.

	• The alarm is reset when the failover is finished successfully, meaning BCT is connected again to the PBX main node or to a PBX fallback node and extension monitors are started. An exception to this is when it involves a SIP@Net Server Cluster failover configuration. Then the alarm is only reset when the BCT is connected again to the PBX main node, the extension monitors are started and also the PBX fallback node is not reachable anymore. • The alarm is also reset when failover support configuration is changed to No.

11.4.3.13. Failover or Failback not successfully completed [2131]

Alarm Type	2131
Description	Automatic or manual failover or failback did not complete successfully.
Severity	Error
Explanation	Automatic or manual failover or failback did not complete successfully.
Additional Info	PBX identification, Failure details.
Required actions	• Check the status of the PBX nodes on the PBX and take proper actions to make the required PBX node available again. • When the failure occurred on a manual or scheduled failover or failback, manually retry the failover or failback action. • The alarm is reset on the first successful failover action. • The alarm is also reset when failover support configuration is changed to No.

11.4.3.14. Soft Queue Alarm [2201]

Alarm Type	2201
Description	PBX Alarm - Soft Queue error
Severity	Error
Explanation	A device configured for use as soft queue device cannot be used as such.
Additional Info	Soft Queue, Device, SIP server address information
Required actions	• Check if the device is available in the PBX. If not, adapt the configuration (with BCT Supervisor Dashboard) or configure the device in the PBX. After the adaptations the system will recover automatically.

11.4.3.15. Maximum number of CTI connections reached Alarm [2202]

Alarm Type	2202
Description	PBX Alarm - Maximum number of CTI connections reached
Severity	Error
Explanation	A new connection cannot be established because the maximum number of CTI connections is already reached.
Additional Info	PBX name, PBX IP address
Required actions	• Check the number of established CTI connections on the PBX and find out who uses them. If there are other (non-BCT) applications consuming resources, stop these applications. After the adaptations the system will recover automatically. • If all applications using CTI resources are required, consider to increase the number of available CTI connections on the PBX.

11.4.3.16. PBX License Alarm [2301]

Alarm Type	2301
Description	PBX Alarm - PBX license problem

Severity	Error
Explanation	An action towards the PBX could not be completed because the PBX did not have the proper (amount of) licenses.
Additional Info	PBX name, PBX IP-address, PBX license
Required actions	• Check the licenses in the PBX. Adapt the licenses if required. The system will recover automatically. • Check options and boundaries in the PBX. • If the licenses in the PBX are not adapted, the system continues working but some actions (like call setup) will fail.

11.4.3.17. PBX Synchronization Alarm [2401]

Alarm Type	2401
Description	PBX Alarm - PBX synchronization problem
Severity	Error
Explanation	Problems were encountered during synchronization of the PBXs.
Additional Info	PBX name, PBX IP address
Required actions	• Check the properties of the PBX in System Settings – Connectivity. If there is any incompatibility between the configuration and the PBX, adapt the settings. Start synchronization. • On error 118,117 'PBX network/cluster missing' then: - When BCT was upgraded to 6.x, check upgrade log files for errors. • On error 119 'Unit number not unique' you have add 1 or more PBX with the same unit number into a PBX network, remove the PBX's from the PBX network or reconfigure the PBX's in the PBX network to have unique unit numbers. Start synchronization. • On error 120 'Cluster ID mismatch' check your PBX configuration. After correction, start synchronization. • On error 121 'configuration file invalid' check the PBXConfigurationService.WinService.exe.config for missing key, invalid IP addresses or not well formatted XML. After correction, start synchronization. • On error 228 'Hotel mode settings don't match' then either: - Correct the hotel mode setting in the PBX or - Correct the product's hotel mode setting. • On error 229 'Station number length setting is not supported' then: - Adjust the station number length setting in the PBX, all station lengths 1..5 must be set to allowed. For SV8500/SV9500 use the following command to correct the setting: ASYD, SYS=1, Index=16. Valid values are '1F' and '3F' • On error 230 'Can only sync via NCN' check that the PBX you are connected to is an NCN (FPC=1) or in a non fusion network also FPC=0 is allowed. Correct it and start synchronization. • If no incompatibility is found: - set Diag@Net tracing (template: Server - PBX Synchronization.dtf) - start synchronization

	- check the result of the synchronization. If the synchronization is not completed correctly, contact the Helpdesk.

11.4.3.18. Non Fatal PBX Synchronization Alarm [2402]

Alarm Type	2402
Description	PBX Alarm – Non fatal PBX synchronization problem
Severity	Error
Explanation	Problems were encountered during synchronization of the PBX, but synchronization is continued but with errors.
Additional Info	PBX name, information about encountered problem.
Required actions	BCT will work but some settings could be missing, e.g. PBX version number, 1 or more extensions/users/groups/groupmembers/facilities. You can find what's missing in the additional info. • On error 106 'stored MarkAllEntriesAsTBR procedure failed', indicates that no deletion of entries in the database will take place during a sync. So the database still contains old/updated and new entries after a sync. • On error 111 'stored deleteAllUnusedEntries procedure failed', all database entries that should be deleted during a sync are not deleted. So the database still contains old/updated/new entries after a sync. • On error 406 'user not send to Directory Browser Web Service', check if IIS is running or restart ISS and start synchronization. • On error 409 'directory sync service failed', check if Directory Sync Service is running or restart Directory Sync Service and start synchronization. • - set Diag@Net tracing (template: Server - PBX Synchronization.dtf) - start synchronization - check the result of the synchronization. If the synchronization is not completed correctly, contact the Helpdesk.

11.4.3.19. PBX Synchronization Command Execution Alarm [2403]

Alarm Type	2403
Description	PBX Alarm –PBX synchronization command execution problem
Severity	Error
Explanation	Problems were encountered during synchronization of the PBX while sending commands to the PBX in order to retrieve data from PBX.
Additional Info	PBX name, information about PBX command that caused the problem.
Required actions	• Check the properties of the PBX in System Settings – Connectivity. If there is any incompatibility between the configuration and the PBX, adapt the settings e.g. PBX type. Start synchronization. • Check if PBX is configured correctly concerning the PBX command that has failed. If no incompatibility is found: - set Diag@Net tracing (template: Server - PBX Synchronization.dtf) - start synchronization - check the result of the synchronization. If the synchronization is not completed correctly, contact the Helpdesk.

11.4.3.20. SQL Server connection Alarm [3101]

Alarm Type	3101
Description	Database Alarm - SQL Server connection problem
Severity	Error
Explanation	There are problems with the connection to the SQL Server which did not recover automatically.
Additional Info	-
Required actions	• If the database is on a remote SQL server, check the connection with the remote server (PING). If there is no connection, re-establish the connection. The system will recover automatically. • Check if the SQL server is running. If not, start the SQL server. The system will recover automatically. • Check if the database is accessible. Check the password of the user 'sa'. Check if the required logins and users are available. If not, configure logins and users. The system will recover automatically

11.4.3.21. SQL Server transaction log full Alarm [3201]

Alarm Type	3201
Description	Database Alarm - SQL Server transaction log full
Severity	Warning
Explanation	The transaction log of the SQL server is larger than the limit as specified in the configuration file (C:\Program Files(x86)\Common Files\NEC\Services\ MonitoringService.WinService.exe.config). The default value is 50MB.
Additional Info	-
Required actions	• Shrink the SQL server transaction log. NB: if there is still enough disk space (no disk space alarm) you may postpone this action until after busy hours. Usually no further actions are required. If you perform the action during busy hours, it is advised to restart the NEC UCSRuntime Service afterwards.

11.4.3.22. BCT Dongle could not be read Alarm [4101]

Alarm Type	4101
Description	BCT License Alarm - BCT dongle could not be read
Severity	Error
Explanation	The system cannot read the BCT Dongle or the fingerprint of the dongle is not correct.
Additional Info	-
Required actions	• Check if the dongle is present on the server. If not, re-insert the dongle. • If the dongle was already present on the system, open the License Manager and check the fingerprint. After the corrections the system must be rebooted.

11.4.3.23. License file cannot be read from External License Server Alarm [4102]

Alarm Type	4102
Description	BCT License Alarm - License file could not be loaded

Severity	Error
Explanation	The system cannot read the license file from the External License Server.
Additional Info	-
Required actions	• Check network connectivity (and if PBX is alive) • Check with License Manager the External License Server connectivity settings. After the corrections the system must be rebooted.

11.4.3.24. License file cannot be read (Japanese) [4103]

Alarm Type	4103
Description	BCT License Alarm - License file could not be loaded
Severity	Error
Explanation	The system cannot read the license file (Japanese Domestic Licensing)
Additional Info	-
Required actions	• Re-load and re-activate the License file After the corrections the system must be rebooted.

11.4.3.25. LMC grace Period Expired [4104]

Alarm Type	4104
Description	BCT License Alarm – Grace Period expired
Severity	Error
Explanation	The licenses are not valid anymore, because the grace period is expired due to connection loss with LMC.
Additional Info	-
Required actions	• Check network connectivity (and is LMC alive and/or is PBX connected to LMC alive) • Check with License Manager the External License Server connectivity settings. After the corrections the system must be rebooted.

11.4.3.26. LMC version incorrect [4105]

Alarm Type	4105
Description	BCT License Alarm – LMC version incorrect
Severity	Error
Explanation	LMC version is incorrect. LMC version must be equal to or higher than 4.0.0.
Additional Info	-
Required actions	• Check LMC version on connected LMC. If version lower than 4.0.0, upgrade LMC.

11.4.3.27. License file is not activated (Japanese) [4801]

Alarm Type	4801
Description	BCT License Alarm - License not [yet] activated
Severity	Warning
Explanation	The system has detected that the license file has not yet been activated. (Japanese Domestic Licensing)
Additional Info	-
Required actions	• Use the Configuration Wizard or License Manager application to activate the license file within the expiration time to prevent system degradation.

11.4.3.28. Multiple Clients Logged Out Alarm [5101]

Alarm Type	5101
Description	BCT Resource Alarm – Multiple clients have been logged out due to inactive state.
Severity	Error
Explanation	When many clients become inactive in a short period of time, this might indicate a network problem.
Additional Info	Number of clients that have been logged out. IP-addresses of clients that have been logged out.
Required actions	• Check the IP-addresses of logged-out clients; this might give an indication about problems in a network segment. • Check the network status with network tools.

11.4.3.29. Queue Level too high Alarm [5201]

Alarm Type	5201
Description	BCT Resource Alarm - Queue level too high
Severity	Error
Explanation	Events from the PBX are not handled fast enough. Probably a performance problem.
Additional Info	-
Required actions	• Check that UCS is running. If not, start UCS manually. The system will recover automatically. • Check the system performance with the Windows Performance monitor (Administrative Tools- Performance). If there are other (non-BCT) applications consuming resources, stop these applications .The system will recover automatically. If there are BCT processes causing high load on the system, please contact the Helpdesk.

11.4.3.30. VMP Service connection Alarm [6110]

Alarm Type	6110
Description	BCT Configuration Alarm - VMP Service connection problem
Severity	Error
Explanation	UCS Runtime Service (VMP-module) cannot start communication towards the VMP Service. - Invalid communication settings? - VMP Service is not running?
Additional Info	-
Required actions	• Check (with Windows SCM) that VMP Service is running. If this is not the case, restart it. • Check (with BCT Supervisor Dashboard) that the communication settings are correct. If not, adapt the settings. When a configuration error is repaired, please restart both VMP Service and BCT.

11.4.3.31. VMP Service sub-system connection Alarm (Protims only) [6111]

Alarm Type	6111
Description	BCT Configuration Alarm - VMP Service sub-system connection problem (PROTIMS only – so SV8300/SV9300 or SV8500/SV9500)
Severity	Error

Explanation	VMP Service cannot contact the SIP/PDS Proxy Service or VMP Service cannot contact the PDS Service.
Additional Info	-
Required actions	VMP Service cannot contact the SIP/PDS Proxy Service: • Check (with Windows Service Configuration Manager) if SIP/PDS Proxy Service is running VMP Service cannot contact the PDS Service: • Check (with Windows Service Configuration Manager) if PDS Service is running General: • Check (with BCT Supervisor Dashboard) the communication settings and make sure that there is no IP-port conflict with other installed applications. If any conflict is found, adapt the settings. • It can be that only one VMP port cannot be opened, while the others do work correctly. • Check if the network port/firewall setting assigned to the VMP port can be used (e.g. by using a SIP phone). When all sub-systems are started again, BCT should recover automatically.

11.4.3.32. Exchange Web Service connection Alarm [6112]

Alarm Type	6112
Description	Exchange Web Service connection problems
Main category	BCT Configuration problem
Sub category	Connection problem
Severity	Error
Explanation	BCT cannot contact the Exchange Server Web Service.
Additional Info	-
Required actions	Use OAuth2 Authentication is not checked: BCT cannot contact Exchange Web Service: • If connection URL cannot be resolved then: ○ Check the Exchange auto discovery service or ○ Check the settings in System Settings, Miscellaneous. • If access has been denied (e.g. http 401 error) then check the NT authentication settings ○ Check the NT user account setting in System Settings, Miscellaneous. Use OAuth2 Authentication is checked: • Check whether the Tenant-Id, Client-Id and Client-secret have been entered correctly in System Settings, Miscellaneous. When all settings are correct, BCT should recover automatically.

11.4.3.33. UCS Runtime License Alarm [6301]

Alarm Type	6301
Description	BCT Configuration Alarm - UCS Runtime License problem
Severity	Error
Explanation	UCS Runtime cannot start because the proper licenses are not present or the license manager cannot be contacted.
Additional Info	-
Required actions	• Check if service LM2Admin is running

	• Check the configuration of the LM2Admin: - PostOfficeIP: IP address of BCT Server - PostBoxPort: the default port is 51870 • In all other cases, please contact the Helpdesk. When a configuration error is repaired, please restart UCS Runtime Service

11.4.3.34. VMP (media port) License Alarm [6303]

Alarm Type	6303
Description	BCT Configuration Alarm – VMP License problem
Severity	Error
Explanation	Number of used vmp licenses is bigger than number of available licenses.
Additional Info	- Number of used licenses - Number of available licenses
Required actions	• Check the number of available licenses in the Health Monitor and the number of configured VMP ports using the Supervisor Dashboard (Tools / Configuration / Media Ports).

11.4.3.35. Static Licenses Out of Range Alarm [6304]

Alarm Type	6304
Description	BCT Configuration Alarm - Static licenses out of range
Severity	Error
Explanation	Number of configured (static) roles is bigger than number of total licenses for that role.
Additional Info	- Number of licenses that could not be claimed. - The Role for which the licenses are claimed.
Required actions	• Check the number of used licenses in the Health Monitor (this is equal to the configured number of roles for this license). When using a shared license file, check this on all BCT servers that share the license file and add them together to get the total number configured roles for this license). If the number of configured roles is higher than the number of licenses you bought for this role, please contact the Helpdesk. • Or remove the number of roles in the Company Directory of System Settings that could not be claimed.

11.4.3.36. Address / port of UCS Server not found Alarm [6401]

Alarm Type	6401
Description	BCT Configuration Alarm - Address of UCS Server not found
Severity	Error
Explanation	The Monitoring Service cannot read the address of UCS from the registry. The following key must be available in the registry: - HKLM\Software\Philips\UCS Communication\PostOfficeIP - HKLM\Software\Philips\UCS Communication\PostBoxPort
Additional Info	-
Required actions	• If the required registry key is not available; add the key with the following value: - PostOfficeIP: IP address of BCT Server - PostBoxPort: the default port is 51870 • If the required key is available, ensure that it is accessible for the user ‘SYSTEM’. • In all other cases, please contact the Helpdesk.

	When a configuration error is repaired, please reboot the BCT server.

11.4.3.37. CTI configuration file not available Alarm [6402]

Alarm Type	6402
Description	BCT Configuration Alarm - CTI Configuration file not available
Severity	Error
Explanation	The CTI Configuration file is not found, not accessible or the contents is not valid XML.
Additional Info	-
Required actions	• Check that the file 'CTIConfig.xml' is available in the same folder where 'sophocti.exe' resides. Check that the file is accessible for user 'SYSTEM'. • Check that the file 'CTIConfig.xml' contains valid XML. (Load the file in an XML reader like e.g. Internet Explorer.) • To repair the problems: access the settings in the BCT Supervisor Dashboard. This will regenerate the configuration file. • If all above checks do not show an error, please contact the Helpdesk. When a configuration error is repaired, please restart the NEC CTI Service.

11.4.3.38. Endpoint for Directory Service not found Alarm [6403]

Alarm Type	6403
Description	BCT Configuration Alarm - Endpoint for Directory Service not found in UCS runtime service configuration file
Severity	Error
Explanation	The configuration file for UCS Runtime service does not contain an entry for endpoint for Directory Service.
Additional Info	-
Required actions	To repair the problem: • Open UCSRuntime.WinService.exe.config, found in "C:\Program Files (x86)\NEC\UCS-Module\Server" (The path relates to a 64 bit operating system) • Make sure in section configuration/system.serviceModel/client there is a section <endpoint address="net.tcp://localhost:8738/DirectoryService" binding="netTcpBinding" contract="DirectoryService.IDirectoryService" name="DirectoryService"/> • Restart NEC UCSRuntime Service. If all above steps do not clear the alarm, please contact the Helpdesk.

11.4.3.39. Phone Number Conversion Rules Inconsistent [6601]

Alarm Type	6601
Description	BCT Configuration Alarm - Phone Number Conversion Rules inconsistent
Severity	Error
Explanation	The Phone Number Conversion file could not be loaded because of a syntax error.
Additional Info	Phone Number Conversion file name.
Required actions	• Check and correct the syntax of the indicated (XML) file. • Re-install or regenerate the indicated file. When the configuration is repaired, the clients of the Phone Number Conversion will automatically reload the file.

11.4.3.40. VMP Service configuration Alarm [6610]

Alarm Type	6610

Description	BCT Configuration Alarm - VMP Service configuration error
Severity	Error
Explanation	The VMP Service failed due to invalid configuration data provided during startup.
Additional Info	Current VMP Service SIP VoIP client settings
Required actions	• Check the VMP Server SIP VoIP client settings if they are correct. • Check that the above settings do not conflict with another application. E.g. an application that uses the same IP-port (range) as VMP. When configuration is adapted, please restart the VMP Service. BCT will automatically recover.

11.4.3.41. VMP Service IP Port configuration Alarm [6611]

Alarm Type	6611
Description	BCT Configuration Alarm - VMP Service IP Port configuration error
Severity	Error
Explanation	The VMP Service failed because the configured IP port(s) is/are already in use by another application(s).
Additional Info	Current VMP Service SIP VoIP client settings
Required actions	Check there is no IP port conflict by another applications for the next VMP configuration items: • BCT Server Local Port (it is suggested to use "0" as port for automatic allocation) • BCT Server RTP Base Port (VMP allocates 384 ports starting from given base port) When configuration is adapted and BCT Server is not restarted, please restart the VMP Service manually. Note: Use the "`netstat -a -b -p udp`" command from the Command Prompt to get an overview of IP port usage of applications.

11.4.3.42. Directory Synchronization Service configuration error [6612]

Alarm Type	6612
Description	BCT Configuration Alarm - Directory Synchronization Service configuration error
Severity	Error
Explanation	The Directory Synchronization Service configuration file could not be loaded because of a syntax error.
Additional Info	Directory Synchronization Service configuration file name
Required actions	• Check and correct the syntax of the indicated (XML) file. • Re-install or regenerate the indicated file. When configuration file is updated and BCT Server is not restarted, restart the Directory Synchronization Service manually.

11.4.3.43. Reporting Service invalid path for saved reports [6613]

Alarm Type	6613
Description	BCT Configuration Alarm - Reporting Service configuration error
Severity	Error
Explanation	The Reporting Service could not save a report to the configured path. Possible reasons: • The configured path for saved reports is empty! • Cannot create folder for saved reports '<path>'!

Additional Info	-
Required actions	- Make sure the save-path folder exists and is accessible. When the save-path is valid, the Reporting Service will save the next report using that path.

11.4.3.44. Reporting Service report save-to-disk error [6614]

Alarm Type	6614
Description	BCT Configuration Alarm - Reporting Service configuration error
Severity	Error
Explanation	The Reporting Service could not save a report to the configured path. Possible reasons: - The configured path is not accessible - There is not enough diskspace. - The Reporting Service is not authorized.
Additional Info	-
Required actions	- Make sure the path to save report is correct and accessible. - Make sure there is enough disk space to save reports. - Make sure the Reporting Service is authorized to save reports to the configured location. When the cause of the problem has been removed, the alarm will be reset when the next report that is successfully saved to disk.

11.4.3.45. Reporting Service report email error [6615]

Alarm Type	6615
Description	BCT Configuration Alarm - Reporting Service configuration error
Severity	Error
Explanation	The Reporting Service could not send a report via email. Possible reasons: - The configured email server is not correct, not operational, or not reachable. is not accessible - The email account of the user that created the report is incorrect.
Additional Info	-
Required actions	- Make sure the email server is configured correctly, is operational and reachable. - Make sure the email account of the user who created the report is correct. When the cause of the problem has been removed, the alarm will be reset when the next report that is successfully send via email.

11.4.3.46. Reporting Service report print error [6616]

Alarm Type	6616
Description	BCT Configuration Alarm - Reporting Service configuration error
Severity	Error
Explanation	The Reporting Service could not print a report. Possible reasons: - The configured printer is not correct, not operational, not reachable or not accessible
Additional Info	-

Required actions	- Make sure the printer is configured correctly, is reachable and operational. - You might try to temporary use a different printer or a print-to-file service. When the cause of the problem has been removed, the alarm will be reset when the next report that is successfully printed.

11.4.3.47. UCS component cannot be started Alarm [8401]

Alarm Type	8401
Description	BCT Internal Alarm - UCS component cannot be started
Severity	Error
Explanation	General UCS Runtime error: - UCS Runtime failed to start. - UCS Runtime stopped. The error is caused by a manual action (stop UCS Runtime Service) or by an internal failure in BCT.
Additional Info	‘Start’ or ‘Stop’.
Required actions	- Try to restart the service manually.

11.4.3.48. Start Synchronization error [8402]

Alarm Type	8402
Description	BCT Internal Alarm - Start synchronization error
Severity	Error
Explanation	The PBX Mirror Server could not start the synchronization to the PBX.
Additional Info	-
Required actions	The required actions depend on the error details as described in the error message.

11.4.3.49. Open Web Interface startup error [8403]

Alarm Type	8403
Description	BCT Internal Alarm - Open Web Interface startup error
Severity	Error
Explanation	FrontEnd Service could not start the SignalR host that exposes the Open Web Interface for third-party applications.
Additional Info	-
Required actions	The required actions depend on the error details as described in the error message.

11.4.3.50. BCT Service not running Alarm [8501]

Alarm Type	8501
Description	BCT Internal Alarm - BCT Service not running
Severity	Error
Explanation	An automatically started service is has stopped, and did not automatically restart within due time.
Additional Info	Name of the service.
Required actions	- Check the state of the service in Windows Administrative Tools – Services. If the service is in ‘stopped’ state, restart the service manually. The system will recover automatically. When the Service cannot be started manually, or if this alarm occurs regularly, please start tracing on the service and contact the Helpdesk

11.4.3.51. Software Exception Alarm [8601]

Alarm Type	8601
Description	BCT Internal Alarm - Software Exception
Severity	Error
Explanation	Software Exception
Additional Info	-
Required actions	• Try to restart the NEC CTI Service manually. • If this does not solve the problem, or if the problem occurs regularly, please contact the helpdesk.

11.4.3.52. UCS Runtime Alarm [8602]

Alarm Type	8602
Description	BCT Internal Alarm - UCS Runtime problem
Severity	Error
Explanation	The Unified Contact Server has encountered problems in its operation and did not recover within due time.
Additional Info	-
Required actions	• Check the status of the Unified Contact Server with the UCS Runtime Manager. If any error is shown, Stop and Start the system with the UCS Runtime Manager. • If this does not solve the problem, or if the problem occurs regularly, please contact the helpdesk.

11.4.3.53. CTI Administration Alarm [8701]

Alarm Type	8701
Description	BCT Internal Alarm - CTI Administration error
Severity	Error
Explanation	The CTI Server was not able to create, allocate or delete an object
Additional Info	Object that caused the error
Required actions	• In most cases the problem will be automatically corrected. • If the problem persists, manually restart the NEC CTI Service. • If this does not solve the problem, or if the problem occurs regularly, please contact the helpdesk.

11.4.3.54. Meeting Center Alarm [6113]

Alarm Type	6113
Description	Meeting Center connection problems
Severity	Error
Explanation	The NMC Proxy service cannot connect to the NEC Meeting Center (NMC) to start Collaboration meetings.
Additional Info	The NMC server address and User name.
Required actions	• Check whether the Meeting Center server address, user name and password are correct. • Check whether the server name is resolvable (DNS) from the BCT server. • Check the status of the NMC server and whether the connection between the NMC server and BCT server is operational. • If this does not solve the problem, or if the problem occurs regularly, please contact the helpdesk.

11.4.3.55. “BCT Compliance Recording” Alarm [6114]

Alarm Type	6114

Description	BCT Compliance Recording connection problems
Severity	Error
Explanation	The Unified Contact Server has encountered problems in its operation/connection with the BCT Compliance Recording server(s).
Additional Info	The recorder-name, server address and PBX address If no recorder-name is shown, the BCT Compliance Recording server cannot be reached.
Required actions	• Check whether the BCT Compliance Recording server is resolvable (DNS) from the BCT server. • Check the status of the BCT Compliance Recording server(s) and whether the connection between the BCT Compliance Recording server(s) and BCT server is operational. • Check whether all BCT Compliance Recording processes are running correctly in the BCT Compliance Recording server(s). • If this does not solve the problem, or if the problem occurs regularly, please contact the helpdesk.

11.4.3.56. UCS Runtime Alarm [8603]

Alarm Type	8603
Description	BCT Internal Alarm – VMP Occupancy problem
Severity	Error
Explanation	The Unified Contact Server has encountered that the number of busy VMP lines passed a configured upper threshold level
Additional Info	Upper threshold percentage
Required actions	• When the number of busy VMP lines decreases below the lower threshold level the alarm is cleared • If this alarm occurs often: add more VMP lines or increase the upper threshold level • This alarm is only raised when both upper and lower threshold levels have a value larger than 0

11.4.3.57. UCS Runtime Alarm [8801]

Alarm Type	8801
Description	BCT Internal Alarm – Emergency Number Called
Severity	Error
Explanation	The emergency number was called from an extension while no operators were present (logged-in) in the system
Additional Info	Extension number, User and Location (if available) calling the emergency number
Required actions	• Log-in an operator and handle the emergency call request to contact the caller *Or:* • Handle the emergency call by other means to contact the caller • Without logged-in operators the alarm can be cleared from System Settings health page pressing the button “Cancel All Emergency Calls”

11.4.3.58. Secure Port Binding Alarm [1203]

Alarm Type	1203
Description	General Server Alarm – Secure port bindings configuration error
Severity	Error
Explanation	One or more secure ports have no binding to a certificate.

Additional Info	Port Numbers
Required actions	Try to correct secure port bindings using the 'Server Manager'

12. Appendix B – BCT AND VIRTUALIZATION

12.1. Virtualized Desktop environments

BCT Desktop Clients can be used in Citrix-based virtualized desktop environments.

12.1.1. Citrix

12.1.1.1. General preparations for Citrix Server

Some general configuration aspects for the Citrix server (4.5) to have BCT desktop clients running:

- Install BCT Desktop Client via the dedicated MSI package via DVD autorun menu "Desktop Client (Special)" – see also 9.1.1 Desktop Client - on the Citrix server. Installation has to be done for all users, i.e. command 'change user/install' should be run before the BCT client installation is started.

- Create a group for the Citrix users with the right to use the BCT desktop client application via Citrix.

- Install Acrobat Reader on the Citrix server (to read BCT documentation).

- Configure the Citrix MetaFrame properties for the BCT client.

- Do not configure a session/application time limit on the Citrix server. A time limit will terminate the BCT client if there is no user action. This option is often used to limit Citrix licenses, but is not acceptable for BCT. Unfortunately, a time limit cannot be defined per application.

- Check the correct proxy location for Internet Explorer is defined:

```
[HKEY_CURRENT_USER\Software\Windows\CurrentVersion or
[HKEY_CURRENT_USER\Software\Wow6432Node\Windows\CurrentVersion (64 bit OS)
\Internet Settings]”AConfigURL” (AutoConfigureURL = "…")
```

- Define BCT server name to help the application find the BCT Server name during login:

```
[HKEY_CURRENT_USER\Software\Philips\MyBusiness@Net] or
[HKEY_CURRENT_USER\Software\Wow6432Node\Philips\MyBusiness@Net (64 bit OS)
"ServerName"="<Name of the Business ConneCT server>"
```

- When the BCT client starts a Web link for the first time via the Web directory, which is part of the full directory, the Citrix server will start the Internet Connection Wizard. To prevent the start of this Wizard use the following registry entry on the Citrix server:

```
[HKEY_CURRENT_USER\Software\Microsoft or
[HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft (64 bit OS)
\Internet Connection Wizard] “Completed”=hex:01,00,00,00
```

When SoftGrid is used with “basic load sets”, the .Net Framework security context and BCT server must be seen as local Internet and must be set in this basic load set.

12.1.1.2. Integration aspects in a Citrix environment

When client side integration is used with other applications (Outlook Contact dialing, Outlook Contact popup, Website popup, Basic call API), these applications must be installed in the same virtualized environment.

As such the “Client Integration” package must be installed in the same virtualized environment as the BCT Desktop client. The feature “Call Handling TSP” is required for dialing from Microsoft Outlook.

The “Client Integration” package installs this TSP, but unfortunately that will not work in a Citrix environment, because the TSP will be registered on machine level instead of user level.
Each user must have a unique TSP to solve this issue.

So per user a unique TSP must be registered and for each user in Outlook one unique TSP must be selected. See also Desktop Integrations white paper.

12.1.1.3. Diagnostics in a Citrix environment

When a BCT Desktop Client or a Hotkey Dialer is running in a Citrix or Terminal Services environment, it is not always possible to run the Diag@Net Service. To enable client tracing in such an environment, it is necessary to manually edit the related configuration file:

Desktop Client

1. Install the BCT Desktop Client (see 12.1.1.1 General preparations for Citrix Server point 1)

2. Browse to folder "C:\Program Files (x86)\NEC\Desktop Client"

3. Open the file "DesktopClient.exe.config" in Notepad

4. Find the section <Switches> and set the logging options, For example for exception logging, set value to "Error". For logging all, set value to "Verbose".

5. Find the section <SharedListeners> and change the log-file location from "InitializeData" to for example "C:\temp\DtcOcLogging.txt"

6. Save the config file

7. Start the BCT Desktop application. The log-file will automatically be created and logging output will be written to the specified file.

Hotkey Dialer

1. Browse to folder "C:\Program Files (x86)\NEC\Client Integration"

2. Open the file "HotkeyDialer.exe.config" in Notepad

3. Find the section <Switches> and set the logging options, For example for exception logging, set value to "Error". For logging all, set value to "Verbose".

4. Find the section <SharedListeners> and change the log-file location from "InitializeData" to for example "C:\temp\HotkeyDialerLogging.txt"

5. Save the config file

6. Start the Hotkey Dialer application. The log-file will automatically be created and logging output will be written to the specified file.

12.2. Virtualized Server environments

12.2.1. General

BCT server can run in virtualized server environments, but take the following into account:

- Virtualization may result in a performance penalty. Care should be taken that the system boundaries as specified in the BCT boundary specification document are met. This may implicate that you need to assign more virtual CPU cores to a VM. It is recommended always to start with the most minimal number of vCPUs possible. Even with one vCPU reasonable performance can be obtained. When it is clear that a benchmark test shows that one vCPU is not enough (for instance when vCPU load exceeds 70%), one or more vCPUs must be added in order to achieve acceptable performance.

- When BCT is deployed with SQL Server we advise to deploy SQL server in a separate VM.

- BCT does real-time media/voice processing on the server. Therefore BCT requires real-time performance from the Operating System. Use the whitepapers of the vendor for optimal performance tuning. In general the following guidelines must be met:

  - Make sure that the VM running the BCT Server receives enough CPU time. To assure sufficient processor resources, CPU reservations must be made on the hypervisor. This means that there is always the guarantee that the BCT VM receives enough CPU cycles from the hosts CPU resources.

  - Make sure that the VM running the BCT Server receives enough memory resources. To assure sufficient resources, make memory reservations in the hypervisor for the BCT VM, so these resources are excluded from memory overbooking. Not doing so may lead to memory swapping at the host level which may dramatically impact the performance in a negative way.

  Note: *Suspending and resuming VM on a hypervisor level is not supported for BCT. When used, various problems can occur due to date/time mismatches with data in the BCT database and the actual server OS date/time.*

- For accurate time keeping, it is best to configure the VMs OS as an NTP client.

12.2.2. VMware vSphere

VMware vSphere ESX/ESXi version 4.1 or higher is supported on a HW platform with Intel XEON 5530 processor or better.

The following vSphere features are supported:

1. vMotion
2. High Availability protection (HA)
3. Fault Tolerant protection (FT)

To guarantee optimal performance, any guide lines in the “Performance Best practices for VMware vSphere 4.1” (www.vmware.com) relevant for the configuration should be followed. In short, the following guidelines should be taken into consideration:

- USB support either via the host or via some form of USB over network, see 12.2.1 General for details.

- Hyperthreading (or logical processor) can be enabled on the host (BIOS), so VMware can take optimal advantage of it. By enabling hyperthreading (HT), the number of physical cores should be doubled to calculate the number of logical cores that can be assigned to vCPUs. When HT is enabled, the HT core sharing mode should be set to “Internal” for the BCT VM. Not doing so may cause another VM running on the same host to seize the LCPU that is co-located on the same physical core as the LCPU that the BCT VM is using. This will affect performance in a negative way.
- VT technology should always be enabled on the host (BIOS) to support efficient processor handling of VMs
- Make sure that any power saving issues enabled in BIOS are not hampering the performance. If necessary disable any power management in BIOS.
- Disable C1E halt states on the host (BIOS)
- Disable unneeded ports (like unused USB ports)
- Enable NTP time sync on the VMs OS, this is more accurate than the time sync obtained by VMware tools from the host. When an NTP or different time source (e.g. domain controller) is applied, the VMware tools time sync should be completely disabled. See section 12.2.2.1 Timekeeping of BCT in a vSphere virtual environment for instructions.

When assigning vCPUs to a VM it is best to start with the least possible vCPUs, which could be just one vCPU. Each additional vCPU will add to overhead handling by the hypervisor, which means that the hypervisor becomes less efficient in case of multiple vCPUs. So when you benchmark your BCT VM under load conditions, and you find the machine performing well with a vCPU load below 70%, it is recommended to stick to just one vCPU. If, on the other hand, you find 1 vCPU is not sufficient, start adding vCPUs until the required performance is obtained.

In any case CPU reservations must be made on the hypervisor so that the BCT VM receives a guaranteed number of CPU cycles from the hosts CPU resources.

- At least 4 GB of RAM should be assigned to the VM running BCT. This amount of memory should be reserved for the BCT VM and not be used for overbooking purposes.
- The SQL server may or may not be co-located with the BCT VM. When co-located, care should be taken that more resources should be assigned to the VM to fulfill both the needs of BCT and SQL server.

12.2.2.1. Timekeeping of BCT in a vSphere virtual environment

Experience with vSphere 5.1 shows that time keeping and synchronization hierarchy in virtual machines is something that should be paid attention to when designing a virtual infrastructure of which BCT is part of. A few possibilities are described here:

1. The virtual BCT server is part of a windows Active Directory domain
2. The virtual BCT server is part of a windows workgroup

Depending on 1 or 2, certain pitfalls need to be considered.

12.2.2.1.1. BCT as part of a domain

When the (virtual) BCT server is part of a windows domain, it will automatically synchronize its internal clock with the clock of the Active Directory Domain Controller (DC). This is because within an Active Directory network the Kerberos protocol used for secure authentication requires that the time offset between DC and domain member servers (like BCT) should not be larger than 5 minutes (when larger, authentication to the domain will fail).

To guarantee this, Microsoft has made it standard practice that domain member servers automatically synchronize their internal clock to the clock of the DC.

The DC itself should be synchronized from an internet NTP source (e.g. time.windows.com or pool.ntp.org) to be assured of proper time keeping throughout the domain. The following picture illustrates this:

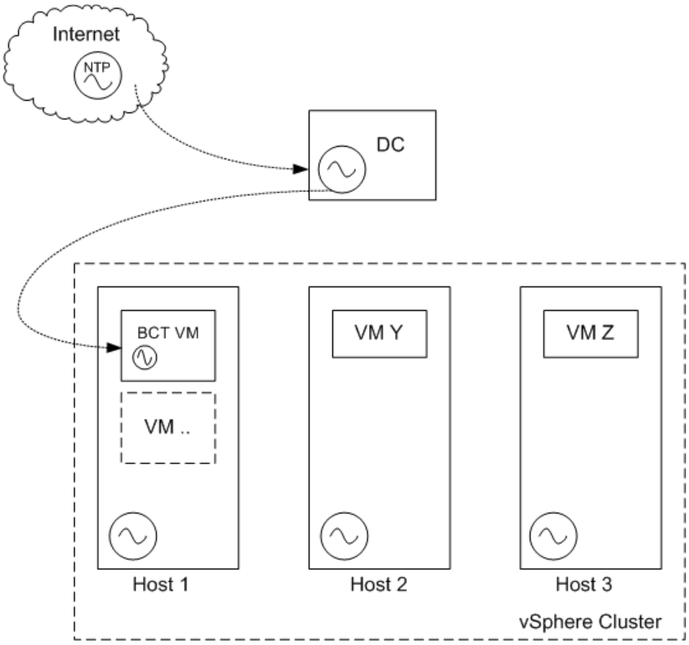


Figure 12-1 Time synchronization in a domain

Step 1: DC synchronizes to NTP source

Step 2: Member server synchronizes to DC.

This time synchronization hierarchy might be simple and straightforward but in the deployment there are a few pitfalls. Most of the time VMware tools will be installed inside the guests OS. One of the advantages of using VMware tools is:

- Time syncing with the host

In this particular case, this becomes a disadvantage. In this particular scenario, when installed, VMware Tools should be told NOT to synchronize the guest’s clock to the host’s clock because the guest VM is already synchronized to the DC clock and there should be only one clock master for the guest.

See 12.2.2.1.3 How to disable time synchronization by VMware Tools

12.2.2.1.2. BCT as part of a workgroup

When BCT is part of a windows workgroup other time synchronization strategies are possible:

1. Synchronize the guest VM(s) directly to an internet NTP source

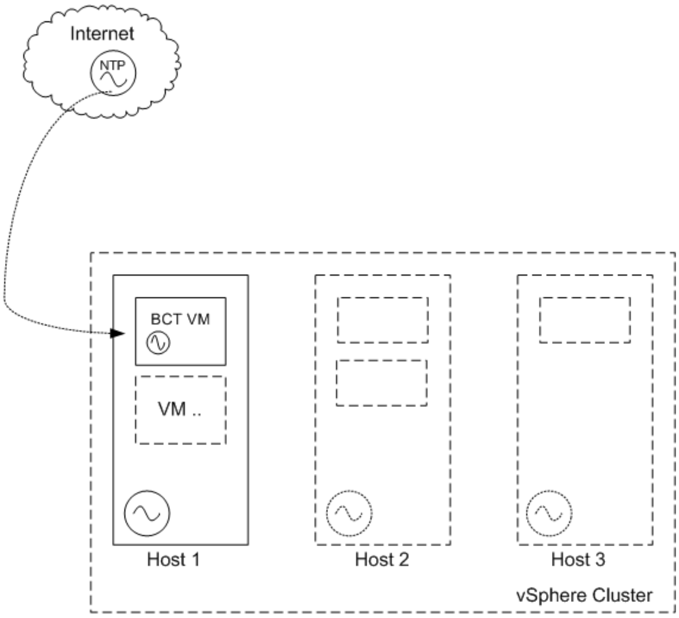


Figure 12-2 Time synchronization in a workgroup

2. In this option, the time synchronization as provided by VMware tools still needs to be disabled because it is conflicting with the chosen time sync hierarchy, see 12.2.2.1.3 How to disable time synchronization by VMware Tools how to do this.

3. Synchronize the hostmachine's clock to an internet NTP source and synchronize the guests to the host.

   In the second case VMware tools synchronization is doing the right thing and can be left on (default setting of VMware tools) and no further time source needs to be configured in the guest OS.

Recommended setting when BCT is part of a workgroup and not in a domain: directly synchronize guest VM to an NTP source. This is more reliable than having VMware tools provide the synchronization.

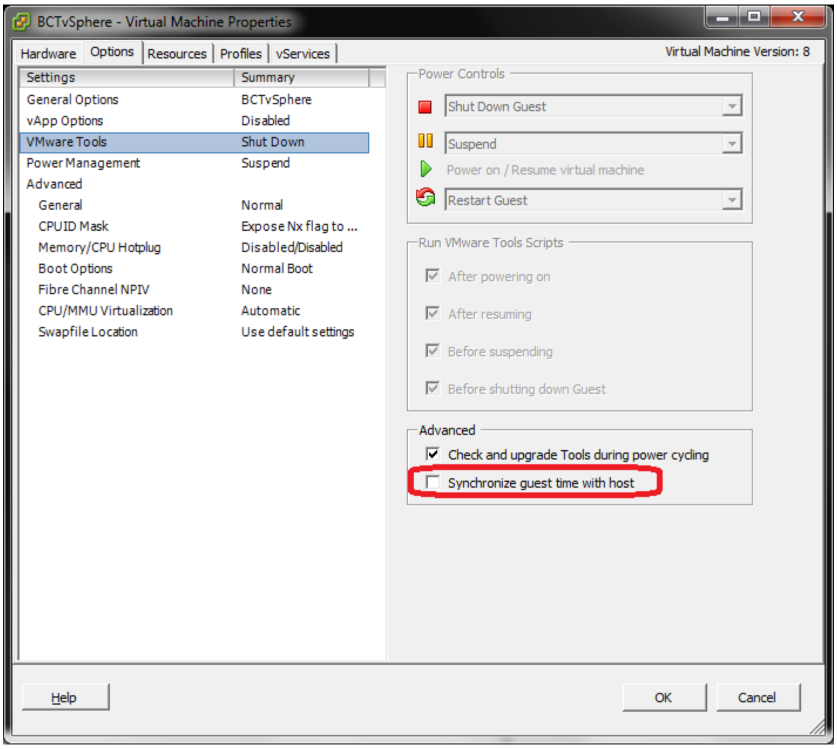
12.2.2.1.3. How to disable time synchronization by VMware Tools

Two actions need to be taken to disable time synchronization.

Disable periodic time sync via vCenter GUI

1. In Access vCenter, Edit VM settings>Options tab>VMware Tools

2. Uncheck "synchronize guest time with host" like in screenshot below.



BCTvSphere - Virtual Machine Properties

Virtual Machine Version: 8

Settings	Summary
General Options	BCTvSphere
vApp Options	Disabled
VMware Tools	Shut Down
Power Management	Suspend
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Power Controls

Shut Down Guest

Suspend

Power on / Resume virtual machine

Restart Guest

Run VMware Tools Scripts

☑ After powering on

☑ After resuming

☑ Before suspending

☑ Before shutting down Guest

Advanced

☑ Check and upgrade Tools during power cycling

□ Synchronize guest time with host

Figure 12-3 Disabling time synchronization in VMware Tools

Set additional configuration parameters for the VM

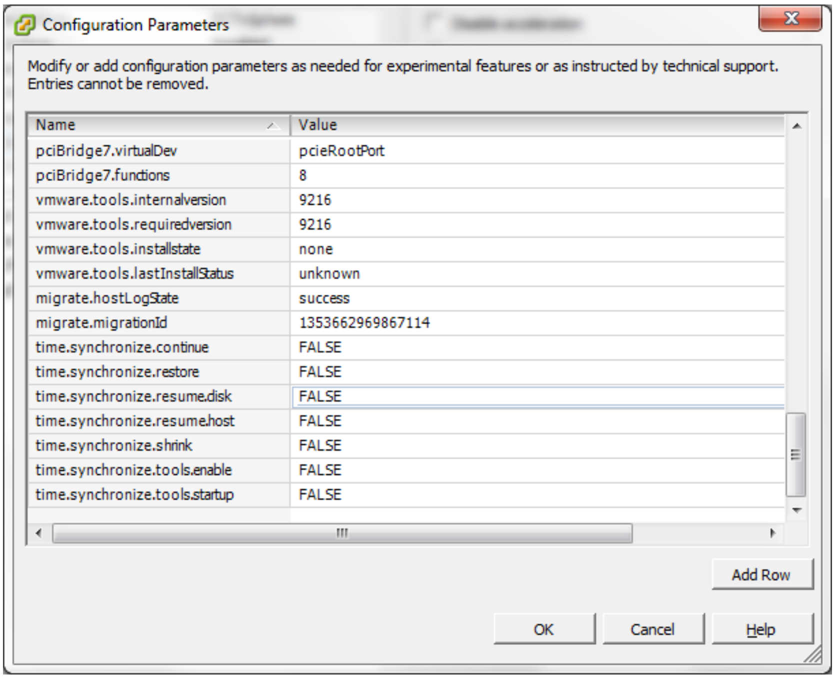
1. Power off the VM

2. Access vCenter, Edit VM settings>Options tab>Advanced>General, now the “Configuration parameters” screen opens.

3. Click “Add row” and add the following lines:

```
time.synchronize.continue = FALSE
time.synchronize.restore = FALSE
time.synchronize.resume.disk = FALSE
time.synchronize.resume.host = FALSE
time.synchronize.shrink = FALSE
time.synchronize.tools.enable = FALSE
time.synchronize.startup = FALSE
```

4. Click OK to confirm and start the VM. See also next screenshot:



Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name	Value
pciBridge7.virtualDev	pcieRootPort
pciBridge7.functions	8
vmware.tools.internalversion	9216
vmware.tools.requiredversion	9216
vmware.tools.installstate	none
vmware.tools.lastInstallStatus	unknown
migrate.hostLogState	success
migrate.migrationId	1353662969867114
time.synchronize.continue	FALSE
time.synchronize.restore	FALSE
time.synchronize.resume.disk	FALSE
time.synchronize.resume.host	FALSE
time.synchronize.shrink	FALSE
time.synchronize.tools.enable	FALSE
time.synchronize.tools.startup	FALSE

Figure 12-4 Entering additional time synchronization parameters

Note: *If the steps above are not taken, VMware tools will continue to try to sync the guest's clock to the host's clock and this is conflicting with the preferred sync hierarchy.*

12.2.3. Microsoft Hyper-V

The general recommendations for virtualization (see 12.2.1 General) should be met.

For optimal performance it is advised not to use the Hyper-V console to access the BCT VM, but rather access it via remote desktop.

12.2.4. Citrix XenServer

Citrix XenServer is supported from version 5.6 SP2 onwards.

Optional the 'Stratus (formely known as Marathon) everRun' high availability solution can be used. Supported version is 6.1.9053.709-HF.EA (hotfix 2) onwards. See 12.2.4.1 Stratus everRun for additional info.

12.2.4.1. Stratus everRun

The Citrix XenServer environment may be protected by 'Stratus everRun' from hardware failures. Only level 2 protection mode (= High Availability) is supported. This means that the active protected virtual machine (PVM) is running on one host, when the host fails, 'Stratus everRun' will boot the PVM on the second (standby) host which then takes over operation.

The general recommendations for virtualization (see 12.2.1 General) should be met.

Note: *It is strongly advised only to perform recovery of a failed host outside of office hours.*

Although BCT functions quite well in 'Stratus everRun' environment and HW failure protection *works very well, there is one downside: bringing up a failed host will cause 'Stratus everRun' to synchronize this host to the one holding the active PVM(s). When local disk storage is used on the hosts this means that PVM disk mirroring will be initiated. Disk mirroring of the virtual hard disks has a negative impact on BCT server performance. In fact during virtual disk mirroring the BCT server is not usable since the host needs almost all resources for the disk mirror activity.*

Tests have shown that this procedure may take 20 minutes to complete.

13. Appendix C – DIRECTORY IMPORT AND EXPORT MAPPING

This chapter describes the mapping between the BCT Directory Fields and the Import/Export Column names. Also the minimum and maximum length is mentioned. Fields are mandatory when the minimum length is greater than 0.

To create an empty import file (template) we advise to do an export from the BCT directory via BCT System Settings. Remove any directory rows that are not required for import.

13.1. Company directory

A BCT Directory Field that has no relation to a column in the import file can only be configured via the BCT System Settings.

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
Absence reason	0	400	Y	Y	N	Y	PBC_AbsenceReason (Not supported anymore)
Account code	0	20	Y	Y	N	Y	accountCode
Address[1]	0	60	Y	Y	N	N	-
Admin rights	1	40	Y	Y	Y	Y	PBC_AdminRights
Agent/Operator Group name	1	20	N	N	Y	Y	AgentGroup[2]
Alternative number	0	25	Y	Y	Y	Y	alternateNumber
Building	0	64	Y	Y	Y	Y	building
Online	Y/N	Y/N	Y	Y	N	Y	Client_Status
Current Port	0	Int	Y	Y	N	Y	Client_Current_Port
Current IP	0	40	Y	Y	N	Y	Client_Current_IP
Calendar	Y/N	Y/N	N	N	Y	Y	CalendarSync
City[3]	0	30	Y	Y	N		-
Company	1	64	Y	Y	Y	Y	CompanyName
Company Id	0	Int	Y	Y	N	Y	CompanyId
Company Privacy	Y/N	Y/N	Y	Y	Y	Y	IsOverrideCompanyPrivacy
pbc_empuser1 ... 20	0	50	Y	Y	Y	Y	PBC_empuser1…20
Custom Y/N 1 ... 20	Y/N	50	Y	Y	Y	Y	PBC_empyesno1…20
Department	1	64	Y	Y	Y	Y	department
Display name	0	16	Y	Y	N	Y	lcdName

[1] Extension property

[2] Comma separated list of groupnames

[3] Extension property

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
Division	1	64	Y	Y	Y	Y	division
Email	0	64	Y	Y	Y	Y	email
Extension Info 1[4]	0	50	Y	Y	N	N	-
Extension Info 2[5]	0	50	Y	Y	N	N	-
Fax	0	25	Y	Y	Y	Y	fax
First name	0	50	Y	Y	Y	Y	FirstName
First name (1)	0	50	Y	Y	Y	Y	FirstName_Synoniem_1
First name (2)	0	50	Y	Y	Y	Y	FirstName_Synoniem_2
Full name	0	120	Y	Y	N	Y	-
Full name (1)	0	120	Y	Y	N	Y	-
Full name (2)	0	120	Y	Y	N	Y	-
Home address line 1	0	60	Y	Y	Y	Y	HomeAddress1
Home address line 2	0	60	Y	Y	Y	Y	HomeAddress2
Home city	0	30	Y	Y	Y	Y	HomeCity
Home phone	0	25	Y	Y	Y	Y	HomePhone
Home state	0	30	Y	Y	Y	Y	HomeState
Home zip code	0	10	Y	Y	Y	Y	HomeZip
Job title	0	40	Y	Y	Y	Y	PBC_JobTitle
Language	0	40	Y	Y	Y	Y	PBC_Language
Last name	0	64	Y	Y	Y	Y	lastname
Last name (1)	0	64	Y	Y	Y	Y	LastName_Synoniem_1
Last name (2)	0	64	Y	Y	Y	Y	LastName_Synoniem_2
License plate 1	0	40	Y	Y	Y	Y	PBC_LicensePlate1
License plate 2	0	40	Y	Y	Y	Y	PBC_LicensePlate2
Location status	0	30	Y	Y	N	Y	locationStatus
Login name[6]	0	20	Y	Y	Y	Y	PBC_LoginName
Lync Uri	0	2048	Y	Y	Y	Y	LyncUri
Mail stop	0	30	Y	Y	N	Y	mailStop
Message count	0	Int	Y	Y	N	Y	messageCnt
Middle name	0	30	Y	Y	Y	Y	MiddleName
Middle name (1)	0	30	Y	Y	Y	Y	MiddleName_Synoniem_1

[4] Extension property

[5] Extension property

[6] There is a limited set of characters that can be used in the login name

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
Middle name (2)	0	30	Y	Y	Y	Y	MiddleName_Synoniem_2
Mobile phone	0	25	Y	Y	Y	Y	MobilePhone
Modem	0	25	Y	Y	Y	Y	modem
Modified display name	Y/N	Y/N	Y	Y	N	Y	lcdNameModified
Multi-Line	Y/N	Y/N	Y	Y	Y	Y	IsMultiLineEnabled
NT login name	0	140	Y	Y	Y	N	PBC_NTLogin
Numeric name	0	16	Y	Y	N	Y	-
Office number	0	25	Y	Y	Y	Y	OfficeNumber
Pager	0	25	Y	Y	Y	Y	pager
Password	0	40	Y	Y	Y	N	password
-	-1	Max Int	N	N	Y	N	-
Personal info	0	400	Y	Y	Y	Y	PBC_PersonalInfo
Phone type[7]	0	2	Y	Y	N	N	-
Photo	0	255	Y	Y	Y	Y	photo
Pin code	0	20	Y	Y	Y	Y	PBC_UsrPinCode
Postal location	0	40	Y	Y	N	Y	PBC_PostalLocation
Primary number	1	16	Y	Y	Y	Y	Extension
Presence	Y/N	Y/N	N	N	Y	Y	Reachability
Presence Name	0	255	Y	Y	N	Y	Reachability_Name
Presence Reason	0	255	Y	Y	N	Y	Reachablity_Reason
Profile Privacy	Y/N	Y/N	Y	Y	Y	Y	IsHiddenWhenBrowsing
Recent IP address	0	40	Y	Y	N	Y	PBC_LastLoginIp
Return time	0	Date	Y	Y	N	Y	returnTime
Roles*	Y/N	Y/N	Y	N	Y	Y	OfficeUser*
State[8]	0	30	Y	Y	N	N	-
Tenant[9]	0	2	Y	Y	N	N	-
Title	0	30	Y	Y	Y	Y	Title
User agent	0	400	Y	Y	Y	Y	PBC_UserAgent
User defined field 1	0	50	Y	Y	Y	Y	userDefined1

[7] Extension property

[8] Extension property

[9] Extension property

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
User defined field 2	0	50	Y	Y	Y	Y	userDefined2
User defined field 3	0	50	Y	Y	Y	Y	userDefined3
Operator additional info (=User defined field 4)	0	50	Y	Y	Y	Y	userDefined4
User identification	0	20	Y	Y	Y	Y	PBC_UsrIdentification
User type	0	Int	Y	Y	N	Y	PBC_UserType
User voicemail access	Y/N	Y/N	Y	Y	N	Y	PBC_UsrUMaAccess
User Web access	Y/N	Y/N	Y	Y	N	Y	PBC_UsrWebAccess
Vip	Y/N	Y/N	Y	Y	Y	Y	Vip
Voicemail	0	25	Y	Y	Y	Y	voiceMail
Wireless	0	16	Y	Y	N	Y	wireless
X400	0	255	N	N	Y	N	-
Zip code[10]	0	10	Y	Y	N	N	-
-[11] **	Y/N	Y/N	N	N	Y	Y	IsPrimaryNumber
-[12] ***	Y/N	Y/N	N	N	Y	Y	IsDisplayedContact
-[13]	Y/N	Y/N	N	N	Y	Y	IsHiddenNumber

Table 13-1 Mappings between Company import/export list and BCT Directory fields

Min Int = -2147483648, Max Int = 2147483647

[10] Extension property

[11] Extension property

[12] Extension property

[13] Extension property

** OfficeUser is a combination of numbers:*

1 for Employee

2 for Agent

4 for Operator

8 not used

64 Voicemail only

128 Phone-based agent

512 Exchange Calendar Integration

1024 = Obsolete (was used for UCC Employee)

4096 for Supervisor

8192 for Essential Employee

16384 Skype for Business Integration

32768 OWI only

Note that ‘OWI only’ cannot be combined with other roles.

Example: *To define a user with the Employee AND Operator role enter ‘5’ (= 1 for Employee + 4 for Operator)*

*** It is possible that there are multiple records for the same user. In that case there is one record with setting ‘IsPrimaryNumber’ is ‘Y’, the other records contain identical information except for the extension field and the ‘IsPrimaryNumber’ which has the value ‘N’.*

**** The ‘IsDisplayedContact’ is an extension setting related to the extension. The extension can be edited so that another user is selected as Displayed Contact.*

13.2. External directory

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
Account	0	30	-	-	Y	Y	accnt
Address	0	60	-	-	Y	Y	address
Alternative number	0	25	-	-	Y	Y	alternateNumber
City	0	30	-	-	Y	Y	city
Company	1	64	-	-	Y	Y	company
Department	0	64	-	-	Y	Y	department
Email	0	64	-	-	Y	Y	email
Fax number	0	25	-	-	Y	Y	fax
Info 1	0	50	-	-	Y	Y	userDefined1
Info 2	0	50	-	-	Y	Y	userDefined2
Info 3	0	50	-	-	Y	Y	userDefined3
Operator additional info (=Info 4)	0	50	-	-	Y	Y	userDefined4
Job title	0	40	-	-	Y	Y	PBC_JobTitle
Mobile phone	0	25	-	-	Y	Y	mobilePhone
Name	0	50	-	-	Y	Y	name
Name_Synoniem_1	0	50	-	-	Y	Y	Name_Synoniem_1
Name_Synoniem_2	0	50	-	-	Y	Y	Name_Synoniem_2
Primary Number	0	25	-	-	Y	y	aniNum
					Y	Y	callNum*
					Y	Y	displayableNum**
State	0	30	-	-	Y	Y	state
Website	0	128	-	-	Y	Y	WebSite
Zip	0	10	-	-	Y	Y	zip

Table 13-2 Mappings between External import/export list and BCT Directory fields

Note: *A combined search will be performed on ANI, Name and Company fields in the external directory of the Full Directory.*

** use only if the aniNum cannot be used for call-back*

*** use only if the aniNum should not be displayed*

13.3. Personal directory

BCT Directory Field in System Settings	Min	Max	Configurable	Protectable	Importable	Exportable	Import/Export Column name
Added date	0	Date	-	Y	N	N	-
Alternate info 1	0	25	-	Y	Y	Y	alternate1
Alternate info 2	0	25	-	Y	Y	Y	alternate2
Alternate info 3	0	25	-	Y	Y	Y	alternate3
Alternate info 4	0	25	-	Y	Y	Y	alternate4
Alternate info 5	0	25	-	Y	Y	Y	alternate5
Alternative Number	0	25	-	Y	Y	Y	alternateNumber
Assistant	0	25	-	Y	Y	Y	assistant
Business	0	25	-	Y	Y	Y	Business
Business 2	0	25	-	Y	Y	Y	Business2
Company	0	64	-	Y	Y	Y	company
Description	0	60	-	Y	N	N	-
Email	0	64	-	Y	Y	Y	email
Home phone	0	25	-	Y	Y	Y	homePhone
Home phone 2	0	25	-	Y	Y	Y	homePhone2
-	0	80	-	N	Y	N	-
Mobile phone	0	25	-	Y	Y	N	mobilePhone
Pager	0	25	-	Y	Y	Y	pager
Personal info	0	3000	-	Y	Y	Y	PBC_PersonalInfo
Primary number	1	25	-	Y	Y	Y	primaryNumber
Related type	0	Int	-	Y	N	N	-
User first name	0	50	-	Y	Y	Y	PBC_UserFirstName
User first name_ Synoniem_1	0	50	-	Y	Y	Y	PBC_UserFirstName_ Synoniem_1
User first name_ Synoniem_2	0	50	-	Y	Y	Y	PBC_UserFirstName_ Synoniem_2
User surname	0	64	-	Y	Y	Y	PBC_UserSurName
User surname_ Synoniem_1	0	64	-	Y	Y	Y	PBC_UserSurName_ Synoniem_1
User surname_ Synoniem_2	0	64	-	Y	Y	Y	PBC_UserSurName_ Synoniem_2
Voicemail	0	25	-	Y	N	N	-
Wireless	0	25	-	Y	Y	Y	wireless

Table 13-3 Mappings between Personal import/export list and BCT Directory fields

14. Appendix D – HOTEL – PMS INTEGRATION

BCT integrates with any vendor's Property Management System (PMS) that provides guest data according BCT PMS interface. Using a check-in/check-out mechanism, any PMS can send BCT new information about guests, such as their name, language and any other relevant information. PMS Connector components integrate the data. In addition the PMS can also notify BCT that a wake up call to a guest has failed. In that case BCT operators wil receive a Wake-up notification pop-up that includes the Guest Name, Room number, extension number and scheduled wake-up time. With the Call button in the pop-up the operator can call the extension of the guest.

In *hotel mode*, BCT ensures that connected Operators and other users have guest information available during any call to or from the guest's room. The user interface of the guest's phone can be set automatically to the guest's preferred language[14].

***Note**: In hotel mode, you can configure when the terminal language is set. By default, the terminal language is set on every change in the directory and every time the BCT server restarts.*

1. Open the Configuration Manager and select the configuration file "C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config".

2. If you do not want the language set any time when a change occurs while BCT is operational, then find "AlwaysUpdateTerminalLanguage" and set its value to "false".

3. If you do not want the language set any time when the BCT server restarts, then find "UpdateTerminalLanguageOnStartup" and set its value to "false".

4. Press button Save to store the value.

5. Restart the Remoting service.

To configure BCT for use with a Property management System, follow the instructions in the following sections.

14.1. Install PMS connector

For hotel integration, you must install PMS Connector on the BCT server. PMS Connector propagates data from PMS database to BCT United database. To install PMS connector:

1. Insert the BCT product DVD. The **BCT DVD Main Menu** window appears. If not, double click D:\Autorun.exe (where D is the drive letter of your DVD drive).

2. Select 'Property Management System (PMS)' and then **Install**.

3. After wizard introduction, click **Next** to continue.

4. After installation, click **Finish**

14.2. Configure PMS system data

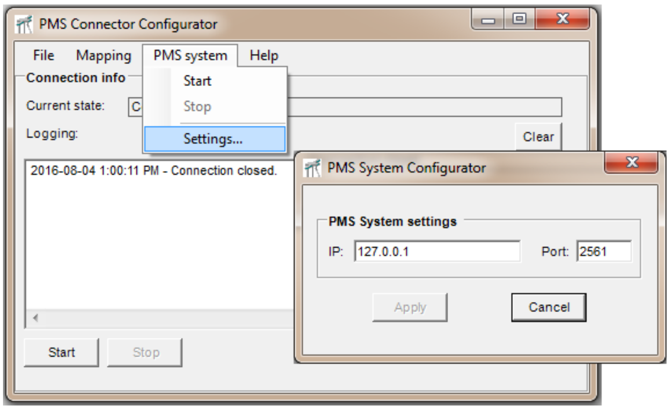
Use PMS Connector Configurator to configure the connection to PMS System:

[14] For Dterm ITR, DTR phones and DTxxx phones, and if language available

1. Open Business ConneCT > Tools > PMS Configurator

2. Go to PMS System > Settings menu to open the configuration window.

3. Enter the IP address of the PMS server, and the port it uses for sending messages, see the following picture.



2016-08-04 1:00:11 PM - Connection closed.

IP: 127.0.0.1 Port: 2561

Figure 14-1 PMS System Configurator - System Settings

An alarm is generated when the connection to the PMS system is lost for some time (PMS system is not available, could be its not running or physical connection is lost); see 11.4.3.2 PMS connection lost [1102].
The time before the alarm is generated after the connection is lost is by default 5 minutes.
This timeout can be changed in the configuration file of the NEC PMS Controller service.

1. Open the file “PMSController.WinService.exe.Config” file, by default located in C:\Program Files (x86)\NEC\PMS Connector\.

2. Find the following line:

```
<add key="AlarmTimeout" value="5"/>
```

3. Change AlarmTimeout field to another value than 5, range is 1 .. 60 minutes

4. Save the file.

5. Restart of the PMS Controller service is not required.

The alarm is cleared when the connection to the PMS system is restored.

14.3. Starting and stopping the PMS connection

To start PMS connection, choose Start from the PMS system menu:

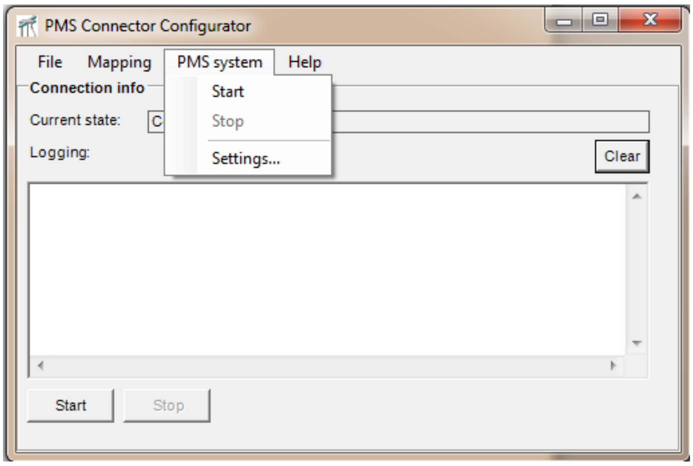


Figure 14-2 PMS Connector Configurator

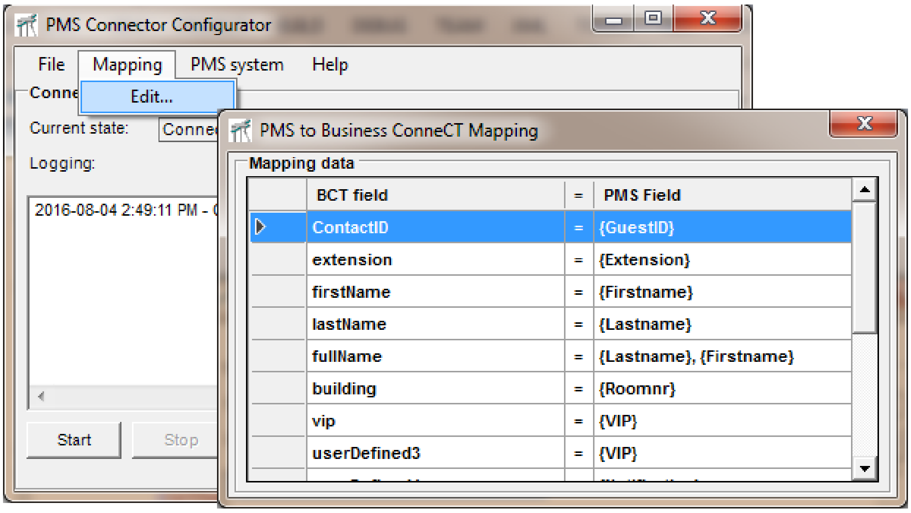
After you start the connection, you can close the PMS Configurator, this does not stop the connection.

To stop the connection, choose Stop from the PMS system menu.

To stop the PMS Controller itself, click Start\Administrative Tools\Services and select 'NEC PMS Controller' and Stop the service. Click on Start to re-establish the connection to PMS.

14.4. Viewing PMS data mapping

To view the mapping between PMS data and BCT fields, choose View from the Mapping menu. By default, you can only view the mapping.



2016-08-04 2:49:11 PM - (

BCT field	=	PMS Field
ContactID	=	{GuestID}
extension	=	{Extension}
firstName	=	{Firstname}
lastName	=	{Lastname}
fullName	=	{Lastname}, {Firstname}
building	=	{Roomnr}
vip	=	{VIP}
userDefined3	=	{VIP}

Figure 14-3 PMS Connector Configurator – View data

14.5. Customizing PMS data mapping

To customize the mapping between PMS fields and BCT fields:

1. Close the PMS Configurator.

2. Open the file “PMSConfigurator.exe.config” file, by default located in C:\Program Files (x86)\NEC\PMS Connector\.

3. Find the following line:

```
<add key="ShowDebugMode" value="0"/>
```

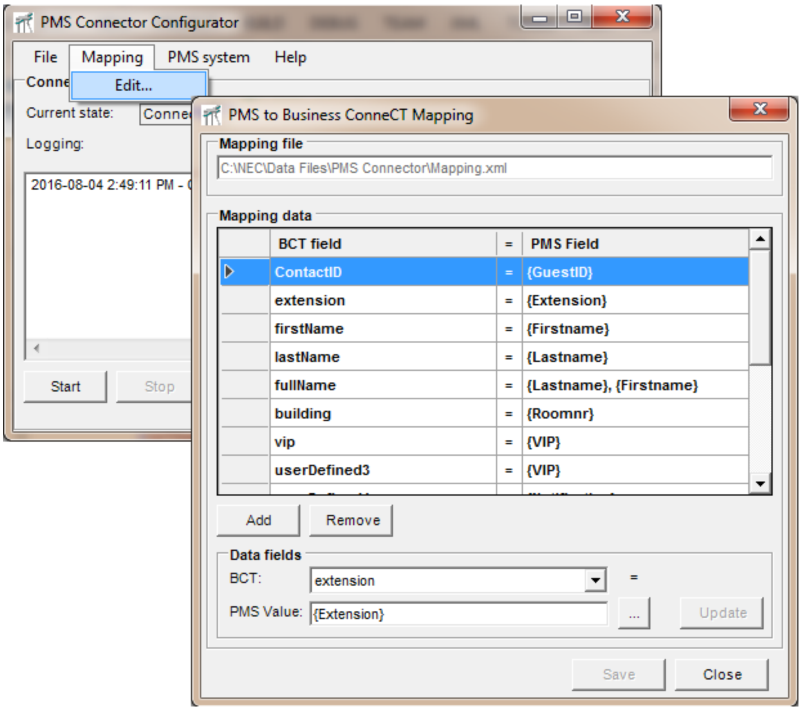
4. Change ShowDebugMode to '1' as follows:

```
<add key="ShowDebugMode" value="1"/>
```

5. Start the PMS Configurator.

6. Select PMS Connector Configurator > Mapping > Edit

You can now edit the mapping table, as shown here:



Mapping file: C:\NEC\Data Files\PMS Connector\Mapping.xml

Mapping data

BCT field	=	PMS Field
ContactID	=	{GuestID}
extension	=	{Extension}
firstName	=	{Firstname}
lastName	=	{Lastname}
fullName	=	{Lastname}, {Firstname}
building	=	{Roomnr}
vip	=	{VIP}
userDefined3	=	{VIP}

Data fields

BCT: extension =

PMS Value: {Extension}

Figure 14-4 PMS Connector Configurator – Edit data

Note: *Changing the standard mapping may affect BCT’s ability to automatically propagate guest data to BCT Operators and users.*

Note: *The ContactID is by default related to the GuestID, but in case of more extenstions on 1 room the GuestID is not unique and must be customized. To make this unique, use the Extension number or a combination of GuestID and Extension number (e.g. "{GuestID}_{Extension}").*

If the ContactID is non numeric, this will be detected and the data will be saved as stringtype in the database.

Note: *If The ContactID is only numeric, then only the last 9 digits will be used.*

By default the column EmpUser20 will be used. If this column is already used, this can be changed in a configuration file:

7. Click Start\Administrative Tools\Services and select ‘NEC PMS Controller’ and Stop the service.

8. Open the file “PMSController.WinService.exe.Config” file, by default located in C:\Program Files (x86)\NEC\PMS Connector\.

9. Find the following line:

```
<add key="EmpUserField" value="20"/>
```

10. Change EmpUserField field to another value than 20

11. Start the PMS Controller service again.

14.6. Registry settings

To activate BCT’s hotel mode, add the following to the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\NEC\ProductSettings\Business ConneCT] or
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NEC\ProductSettings
\Business ConneCT] (64 bit OS)
string value "HotelServer"="1"
```

Note: *This registry setting will be set automatically to Hotelmode when PMS-Connector is installed. A reboot of the server is required.*

14.7. SV8500/SV9500 configuration

Configure the SV8500/SV9500 as described in chapter 4.3 UNIVERGE SV8500/SV9500 configuration with the following differences:

ASYD sys1 index 160
Bit 0=1 Hotel Application is available
Bit 1=1 Hotel service (fixed “1”)
Bit 2=1 Room status memory 24 bytes

ASYD Sys1 index 160 b6=0/1
Number plan for guest is different from administration station / number plan for guest and administration station are the same (usually “1”)

Skip all ASPA commands.

For all ASDT commands, use AAST instead and include additional parameters (Room class, Annex, Ground, Floor)

For all AISTL commands, include additional parameters (Room class, Annex, Ground, Floor)

14.8. SV8300/SV9300password

The SV8300/SV9300 offers the possibility to automatically set the display language of the guest's telephone.

The PBX Config Service is used to set the language of the extension via Maintenance Administration Terminal (MAT). This requires a password with user level 2.
In case of an SV8300/SV9300, PC Pro is used and only a level 7 password is required.

How to enable a password for the SV8300/SV9300

Log onto MAT as level 7 user.

E9 > 9 > 1;	Disable password service.
E9 > 2 > [password];	Enter password
E9 > 9 > 0;	Enable password service

15. Appendix E - BCT SYSTEM RELATED BOUNDARIES

In the BCT Boundary Specification the limits of individual boundaries are specified.

16. Appendix F – OUTLOOK CONTACT POPUP SETTINGS

A couple of system wide setting are available for the Outlook Contact pop-up feature. These can be found in the XML configuration file “C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.exe.config” on the server PC.

PerfectMatch
For an exact match the key PerfectMatch should be changed to true. If set to true, then the search for outlook contacts is done according to an exact match.

ContactSearchFields
This is a comma separated list of contact fields to search in for the to-be-searched number. The order of the fields in the list is irrelevant. The supported fields are:

- PrimaryPhone
- MainPhone
- BusinessPhone
- BusinessPhone2
- Mobile
- HomePhone
- HomePhone2
- CarPhone

If two contacts have a match on the same field (so both are found based on ‘PrimaryPhone’), the ‘Best-Match-Indicator’ (BMI) will decide which contact to show. If both BMI values are the same then both will be shown. This is limited by the value of “MaxContactsDisplayed”.
The BMI value is a calculation based on the relevance of the field and the number match of the field. If for example contact ‘A’ has ‘PrimaryPhone’ = ‘1122’ and contact ‘B’ has ‘PrimaryPhone’ = ‘01331122’ and the number to-be-searched is ‘1122’, contact ‘A’ will have better BMI value then contact ‘B’. This is because contact ‘A’ has an exact match!
Note: It is important to know that this BMI–calculation does not guarantee in showing only the exact contact searched because it strongly depends on the order of the search-results coming from Outlook.

MaxContactsDisplayed
This is the maximum number of contacts shown in one number lookup. This can be set to a different value.
When MaxContactsDisplayed is set to value 0, the Outlook Contact pop-up feature is disabled for all users.

17. Appendix G – BCT USER AUTHENTICATION MODES

BCT supports two user Authentication modes, i.e.:

- Basic Authentication; or
- Integrated Windows Authentication.

A user can login either via *Basic Authentication* or *Integrated Windows Authentication*. Moreover, Integrated Windows Authentication requires that BCT server and client machines are put in the same *Domain-network*.

Basic Authentication

When using *Basic Authentication* (default), the user is authenticated by BCT. For this purpose you have to specify a ***Login Name*** and ***Password*** and confirm that password for every user. Use BCT System Settings to configure these user credentials when adding or updating a BCT user.

When using *Basic Authentication*, any information entered in the fields for *Integrated Windows Authentication* are ignored by BCT.

Note: *For security reasons, BCT generates a random Password for every user added or imported into BCT. To enable a new user to log in, you must first edit the user's password.*

Integrated Windows Authentication

When using *Integrated Windows Authentication*, the user is authenticated by Windows. This means that the BCT user is authenticated with the account he used to log on Windows. When he tries to connect to BCT server, his Windows logon name is sent to BCT Server. If this Windows logon name is known by the BCT Server, then this user is authenticated.

For this purpose you have to specify an ***NT Login name.*** Note that you do not need to specify a (Windows) password for this account when you enter this information in BCT. If BCT is aware of the account you used to logon on the Client machine, BCT assumes that you are already authenticated by Windows.

When using *Integrated Windows Authentication*, any information entered in the fields for *Basic Authentication* is ignored by BCT.

Note: *The login name* specified in the ***NT Login name*** textbox is not the *Fully Qualified Domain Name (FQDN)* for this user – it is the *NetBIOS* user name, which is used by Windows for interoperability with older computers and services.

Example:

Fully Qualified Domain name = UCSLAB.LOCAL
Domain name (Pre-Windows 2000) = UCSLAB

If user ***James*** is added to this domain then he can logon on Windows correctly using any of the following user logon names:

Fully Qualified Domain Name (FQDN) for this user	*UCSLAB.LOCAL\James*

NT Login name for this user	*UCSLAB\James*
Sent to server	*UCSLAB\James*

Choose which user Authentication mode to use

Almost all BCT features support both authentication modes and it is up to your company policy to choose one of the two modes – by default Basic Authentication will be used.

Note: *Currently, “Client Integration” is the only package with features that does not support Basic Authentication. In order to use “Client Integration” you have to use **Integrated Windows Authentication**.*

Note: *BCT Mobile Client, BCT DT XML Client, BCT DT XML Agent, BCT DT XML Employee do not support Integrated Windows Authentication. In order to use these you have to use **Basic Authentication**.*

Change user Authentication mode for *BCT Essential Employee Client*

After you have made a choice about which authentication mode you want to use, you must set the user Authentication mode in BCT as follows:

- Make sure that you specify appropriate user credentials for each user you have defined in BCT – see sections Basic Authentication and Integrated Windows Authentication.

1. Configure IIS to use Integrated Windows Authentication or allow *anonymous access* (in order to support Basic Authentication).

To support Integrated Windows Authentication take the following actions:

1. On the BCT server, start Internet Information Services (IIS) Manager.
2. Expand Web Sites > Default Web Site, and select CA.
3. In Feature View pane, double-click the 'Authentication'-icon.
4. Right-click the **'Windows Authentication'** and select 'Enable'.
5. All others should be set to 'Disabled'.
6. Close the IIS Manager.
7. Edit web.config to change the Authentication mode to “Windows”

To support Basic Authentication take the following actions:

1. On the BCT server, start Internet Information Services (IIS) Manager.
2. Expand Sites > Default Web Site, and select CA.
3. In Feature View pane, double-click the 'Authentication'-icon.
4. Right-click the **'Anonymous Authentication'** and select 'Enable'.

5. All others should be set to 'Disabled'.
6. Close the IIS Manager.
7. Edit web.config to change the Authentication mode to “Forms”

18. Appendix H – DIALING RULES AND NUMBER CONVERSION

18.1. Introduction

18.1.1. Telephone Number presentation

BCT uses Standard Telephone Number format for presentation of telephone numbers:

- Extensions within the company: Only the internal number part (like 2300)
- External numbers: full format (like +31356899111)
- Special numbers: full format (like Dutch alarm number 112: +31112)

18.1.2. Entering Telephone Numbers in directories

When you enter a telephone number in a directory, you should use the Standard Telephone Number format. A Number Completion facility assists you to do that.

BCT can handle telephone numbers in other formats, like local telephone numbers, but this is not recommended because only the standard format is guaranteed to be unambiguous.

Do not enter an outside access code as part of a telephone number. In old systems such numbers still might occur. There are several ways to deal with this issue, see 18.3.1 Number Conversion after upgrade.

18.1.3. Using Telephone Numbers in calls

When BCT uses a telephone number to make a call, the offered number is converted to a dialable number. This is done automatically by Number Conversion, based on Dialing Rules.
See 18.2 Dialing Rules Configuration and 18.3 Number Conversion.

However, it is possible to deactivate Number Conversion for telephone numbers manually entered by the user, via the option "Number Conversion is applied to entered numbers for call setup".
See 8.1.1 Using the Configuration Wizard – step 16.

If this option is activated, then users do not have to enter the complete number. They can enter an internal number, a local number, a national number or an international number. The Number Conversion will automatically add the outside access code and national prefix, if required and complete the number.

If this option is deactivated, then the user must add the required outside access code and national prefix to create a dialable number. Deactivating this option may be required if there is (substantial) overlap between internal numbers and local numbers.

18.2. Dialing Rules Configuration

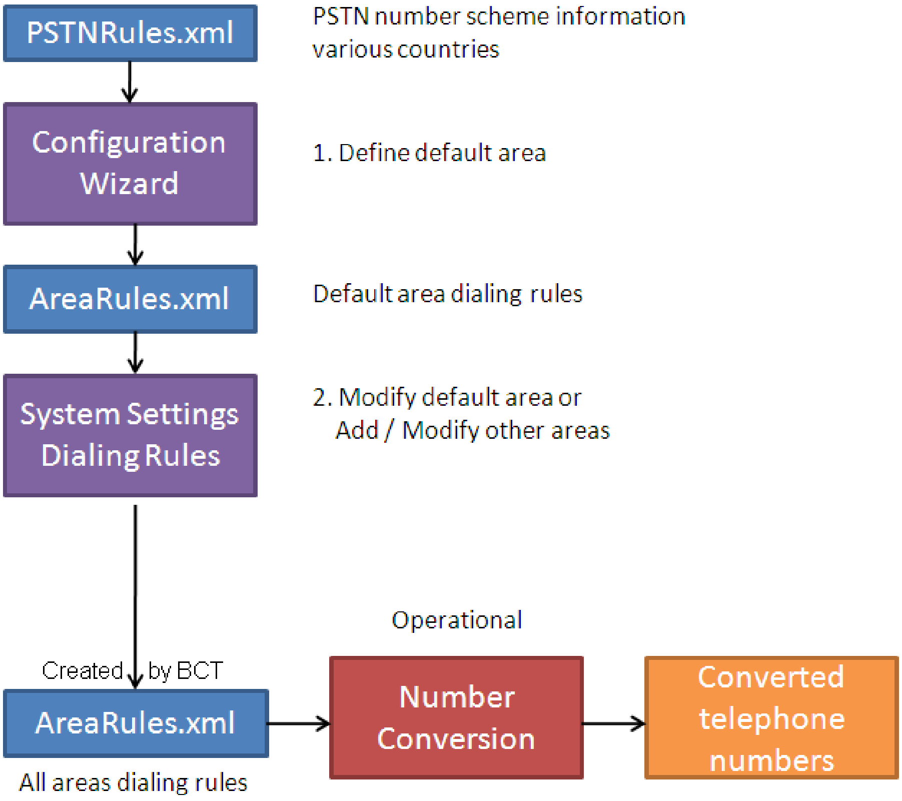
18.2.1. Introduction

To get Number Conversion working correctly, you need to configure the Dialing Rules first. Dialing Rules are entered for a given *area*.

During installation one default area is created, which is applicable for all extensions in BCT. This will be sufficient for most BCT installations. To accomodate more complex requirements, like use of Carrier Codes, you can customize the Dialing Rules for the default area within BCT System Settings.

When you want to configure other Dialing Rules for part of the extensions, you can add more areas. This is done in BCT System Settings as well. After you have created a new area you can assign it to the proper extensions.

18.2.2. Details



1. The PSTN number schemes have been predefined in PSTNRules.xml (delivered with BCT). This file contains country code, international access code, national access code and integrity rules for a number of countries.

   After a new installation Dialing Rules for the default area must be defined with the Configuration Wizard (which uses the PSTNRules.xml file), see 8.1.1 Using the Configuration Wizard – step 16. Or, you can create the Default Area manually, see 8.1.11 Dialing Rules.

   All extensions will automatically be related to the default area.
   For most installations this configuration is sufficient (if all extensions use the same dialing rules).

2. For more complex installations, additional areas can be defined via System Settings / Dialing Rules tab, see 8.1.11 Dialing Rules.

New areas need to be assigned to the proper extensions. See 8.5.1 Extension Configuration (Company Directory) step 5 and 8.5.11 Edit or create a series and/or range of extensions.

You can also assign an area to a PBX. When new extensions are created on that PBX, they will automatically be related to the Default Extension Area of the PBX, after synchronization. Existing extensions are not changed. See 8.1.5 Connection to PBX.

18.3. Number Conversion

BCT uses different telephone number formats on different places: standard format for number storage and display, several dialable formats for calls towards the PSTN, and formats for number recognition.

Conversion between these formats is controlled by the rules which are delivered as part of the BCT package and the Dialing Rules definition per area (see 18.2 Dialing Rules Configuration) .

18.3.1. Number Conversion after upgrade

When you want to upgrade your system from a BCT package older than BCT 5.1, you have to upgrade to BCT 6 first. After this upgrade, and before upgrading to BCT 8.x, you must convert the telephone numbers in your system to standard format using the Phone Number Conversion Update Wizard tool that was delivered with BCT 6.

18.3.2. Trunk Line access codes

You need to do some extra configuration when:

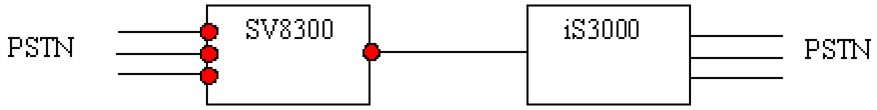
1. you have a PBX network with two or more PBXs
   – AND –

2. the network contains one of the following PBX types:
   - SV8300/SV9300
   - SV8500/SV9500
   - SV8100/SV9100 / AspireX/AspireUX
   - UNIVERGE 3C

– OR –
In case of SV8500/SV9500 with older versions or not programmed TAC.
By default BCT expects that the PBX gives the TAC with the external numbers.

In such configurations the telephone number information from the PBX might have no or wrong outside access code prefix.

Example:



Telephone numbers from or to the marked routes might be presented to the BCT application in the wrong format.

To correct this, please execute the following steps for each PBX of the above listed types:

1. Check whether all trunk routes (CCIS routes!) in the PBX have the same Outside Access Code.

If “YES”: no further configuration is needed for this PBX (configuration has already been done automatically).

If “NO”: go to step 2.

Note: *The CCIS routes between the PBXs might have no Outside Access Code. Configure this configuration as described below, and define an empty Outside Access Code prefix for each CCIS route.*

2. Find the Area of the PBX in the ‘Default Extension Area’ for the PBX, see 8.1.5. Connection to PBX.

3. Go to the Dialing Rules tab and open the edit screen for this Area.

4. The **Outside Access Code(s)** is a comma-separated list; add the Outside Access Codes that are not yet there at the end of the list.

5. With notepad or any XML editor, open the CTI Configuration file ‘CTIconfig.xml’ (by default located in C:\Program Files (x86)\Common Files\NEC\TSAPI Service).

   You will find the default configuration for the PBX that looks like the following example:

```
<PBXConfiguration>
    <PBX IP="192.168.0.1" Type="SV8300">
        <TrunkAccessCode Prefix="0" MaxInternalNumberLength="4" />
    </PBX>
</PBXConfiguration>
```

Adapt these lines to reflect the projecting of the PBX.
An example below (the bold green lines are added):

```
<PBXConfiguration>
    <PBX IP="192.168.0.1" Type="SV8300">
        <TrunkAccessCode Prefix="0" MaxInternalNumberLength="4" />
        <Trunk RouteNr="20">
            <TrunkAccessCode Prefix="9" />
        </Trunk>
        <Trunk RouteNr="50">
            <TrunkAccessCode Prefix="" />
        </Trunk>
    </PBX>
</PBXConfiguration>
```

This configuration means that the Outside Access Code prefix for all trunk routes is ‘0’ except for route 20 (Outside Access Code prefix = ‘9’) and route 50 (no additional prefix required)

Note: *Other attributes than 'Prefix' of the TrunkAccessCode tag (e.g. 'MaxInternalNumberLength') should not be modified.*

Note: *For a CCIS route (XX) handling both calls from internal callers (Access Code not to be added) as well as external callers from PSTN (Access Code to be added), BCT detects the difference between an internal and external number based on the maximum internal number length specified in the Area configuration in System Settings.*

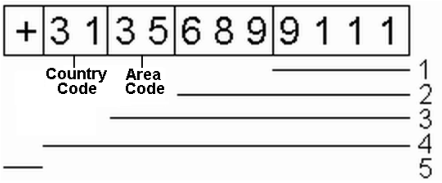
When the calling party number exceeds this maximum, for the calling party the Access Code prefix is added (if defined for the PBX or for the specific route XX) otherwise no Access Code prefix is added.

19. Appendix I – GLOSSARY OF BCT TERMS AND ACRONYMS

1. BCT Contact Center Client	Software package that will install on the client PC, which contains a.o. BCT Supervisor Dashboard.
2. BCT DECT Client	Company Directory browsing capability on DECT handsets. Provides presence and click-to-dial for entries found.
3. BCT Desktop Client	BCT PC client for Operator, Contact center Agent or Employee.
4. BCT DT XML Client	Agent or Employee on a NEC DT terminal.
5. BCT DT XML Agent	Call center Agent functionality on a NEC DT terminal.
6. BCT DT XML Employee	Personal-, Company- and External Directory access, Call log, Voicemail log, all with presence and dialing functionality, Incoming call and Deflect functionality on a NEC DT terminal.
7. BCT Mobile Client	Web based access for certified Mobile phones to Personal-, Company- and External Directory, providing presence and click-to-dial; possibility to set/reset temporary presence.
8. BCT Polycom Client	Anonymous Access to the BCT Company Directory with presence and click-to-dial for a range of Polycom terminals.
9. BCT Supervisor Dashboard	A tool kit with a flexible and user-friendly interface for Administrator, PBX engineer or Supervisor, which can be used to either • configure part of the system; • build a Call Flow; • monitor the Contact Center behavior; • generate statistical reports; • manage wallboard information; • manage agents and groups. By creating login accounts with certain privileges, an administrator can control whether supervisors can use more or fewer functions.
10. Call Flow	A call flow is a collection of call flow modules. The modules are linked and from that moment on we talk about a call flow. The call flow guides the call / caller trough the linked call flow modules.

	A caller dials the number of the BCT Contact Center. The PBX is configured in such a way that the caller will be connected to one of the IVR lines, the so-called Starter Lines. A call flow always starts with a starter module. The starter module specifies the IVR lines that are used as Starter Lines and the next module in the call flow when entering those Starter Lines. From the starter the call is transferred to the next module. With the successive call flow modules you can automate and customize how calls are handled by the BCT Call Center.
11. Configuration Wizard	A quick configuration tool used for initial configuration of BCT for a stand-alone PBX with a single operator and or a simple straightforward Contact Center
12. Directory Browser	The BCT web application for BCT users, providing separate tabs for personal-, company- and external phonebooks, as well as management of a user's personal properties.
13. Fallback	With fallback we refer to alternatives for a functionality, connection or device in case of break down. Please refer to the document on BCT fallback scenarios on the support pages for extra information and remedies.
14. IVR configuration	Calls are queued on an VMP line group. Voicemail and announcements are played via Dialogic boards or VMP in the BCT server. IVR configuration must be used in case the Call Flow contains interactions with the caller, and uses Call Flow modules where lines are needed during the whole call life time: • Voicemail • Auto Attendant • Option Menu • Identification with PID
15. IVR less configuration	In an IVR-less configuration, no Dialogic or VMP lines are reserved for the Call Flow. Calls are queued on Routing Points and not on VMP lines. This can always be used for: • Routing to group of agents • Identification with dialing or dialed number • Outbound service without announcements etc. However, an IVR-less Call Flow can 'borrow' existing VMP lines to use it shortly when needed, for instance • To play Queue announcements • To play Outbound announcements etc.

	Situations where there is no response from / interaction with the caller. ***Note:*** *In a system without VMP lines, some announcements in Queue are still possible via the PBX.*
16. Location Diversity	A PBX feature of the SV8500/SV9500. It takes care of automatic takeover of most of the PBX functionality between PBXs in case of failure of one of them (including numbers). The PBXs may be located on different geographic locations.
17. Monitored number	Extensions in the PBX of which all the activity is signaled to applications (eternal to the PBX). And on top of that these applications can control those extensions and set up or answer calls or (re)set forwardings on behalf of those extensions.
18. Queue	A Queue is a number in the PBX (a Routing Point or Virtual extension), or a telephone-line registered on the BCT server where multiple calls can be positioned while they are not (yet) connected to actual telephones. Depending on the status of the BCT clients or the telephones in the company, BCT moves these calls between the Virtual extensions (queues) and extensions with actual telephones.
19. Routing Point	A virtual number that is monitored by BCT. Calls are queued on these virtual numbers until they are handled by BCT.
20. Starter Line	A starter line represents a number or range of numbers. When that number (or a number in the range) is called, then the call enters the Call Center in the related Starter Module (the starting point of a Call Flow).
21. Synchronization	An activity of the BCT server to retrieve extension data from the PBX. It comprises a.o. the extension numbers, forwarding status and extension type. This data is used to assist the engineer or administrator in configuration of the BCT system.
22. BCT System Settings	A Web application where you can manage users and directory entries, PBX connectivity, the BCT health status and other system wide settings.
23. Virtual extension	An extension in the PBX that is used by BCT to create certain functionality. These extensions have all the capabilities of a 'normal' extension, but do not have a real telephone connected.

	BCT uses these extensions especially for creating Queue functionality in the PBX.
24. Standard Telephone Number format	The standard format for internal numbers is DNR. The standard format for external numbers is E164. An E164 number typically contains the following elements (not all elements are applicable in all countries):  + 3 1 3 5 6 8 9 9 1 1 1 Country Code Area Code 1 2 3 4 5 1. Internal number (within the company) 2. Local number (within the area) 3. National number (within the country) 4. International number 5. International prefix
25. BCT Essential Employee Client	For the Employee role, a web client is also available, called "BCT Essential Employee Client". This client supports Directory Search, managing Personal Directory, Call Forwarding settings, SMA settings, ACD Group presence and DND settings.
26. Configuration Manager	A tool to modify the value's of key's in BCT configuration files. For details see Appendix T - Configuration Manager
27. Geographic Redundancy	A PBX feature of the SV9500. It takes care of automatic takeover of all of the PBX functionality between PBXs in case of failure of one of them (including numbers). In contrary of location diversity where all PBX's can be active at the same time, with Geographic redundancy always one PBX is active while another is standby (or not active at all).

20. Appendix J – Open Source and Third Party Software

The Business ConneCT product also includes code written by other third parties. Additional details regarding these and other third party code included in this product, including applicable copyright, legal, and licensing notices, are available below.

For third party code that is changed by NEC Nederland B.V. the source code can be obtained “as-is” by sending a written request to:

NEC Nederland B.V.
P.O. BOX 32
1200 JD Hilversum
The Netherlands

Note that the delta ‘Δ’ column indicates whether code changes have been made by NEC.

Name	Version	Notice / Terms	Δ
AngularJS Project homepage 🔗	1.2.29	Copyright Google, Inc. Licensed under terms of MIT License 🔗	Y
Behaviors.Forms Project homepage 🔗	1.4.0	Copyright David Britch Licensed under terms of MIT License 🔗	
Corcav.Behaviors Project homepage 🔗	2.3.7	Copyright Maksim Volkau. Licensed under terms of MIT License 🔗	
Dapper.StrongName Project homepage 🔗	1.50.2	Copyright Stack Exchange, Inc. Licensed under terms of Apache 2.0 🔗	
dmidecode Project homepage 🔗	2.9	Copyright Free Software Foundation, Inc. Licensed under terms of GPLv2 🔗	
EntityFramework Project homepage 🔗	6.4.4	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Expat XML Parser Project homepage 🔗	2.2.9	Copyright Thai Open Source Software Center Ltd and Clark Cooper Licensed under terms of MIT License 🔗	
Google.Apis Project homepage 🔗	1.45.0	Copyright Google Inc. Licensed under terms of Apache 2.0 🔗	
Google.Apis.Auth Project homepage 🔗	1.45.0	Copyright Google Inc. Licensed under terms of Apache 2.0 🔗	
Google.Apis.Core Project homepage 🔗	1.45.0	Copyright Google Inc. Licensed under terms of Apache 2.0 🔗	
gSOAP Toolkit Project homepage 🔗	2.8.93	Copyright R. van Engelen, Genivia, Inc. Licensed under terms of GPLv2 🔗	
jQuery Project homepage 🔗	1.5.1 1.8.2 1.10.2 2.2.4 3.4.1	Copyright jQuery Foundation a.o. Licensed under terms of MIT License 🔗	
jQuery UI Project homepage 🔗	1.8.2 1.10.3	Copyright jQuery Foundation a.o. Licensed under terms of MIT License 🔗	
Krypton OutlookGrid Project homepage 🔗	1.2.0	Copyright JDH Software Licensed under terms of Ms-PL 🔗	Y
Krypton Suite Project homepage 🔗	4.5.0	Copyright Phil Wright Licensed under terms of BSD-3 🔗	Y
log4net Project homepage 🔗	2.0.8	Copyright Apache Software Foundation Licensed under terms of Apache 2.0 🔗	

Name	Version	Notice / Terms	Δ
MailKit Project homepage 🔗	2.10.1	Copyright .NET Foundation Licensed under terms of MIT License 🔗	
Microsoft Exchange Web Services Managed API Project homepage 🔗	2.2	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	Y
Microsoft.AspNet.Cors Project homepage 🔗	5.2.3	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNet.Identity.Core Project homepage 🔗	2.2.1	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNet.SignalR.Client Project homepage 🔗	2,3,0 2.4.1	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNet.SignalR.Core Project homepage 🔗	2.4.1	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNet.SignalR.JS Project homepage 🔗	2.4.1	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNet.WebApi.Client Project homepage 🔗	5.2.6	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNet.WebApi.Core Project homepage 🔗	5.2.3	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNet.WebApi.Cors Project homepage 🔗	5.2.3	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNet.WebApi.WebHost Project homepage 🔗	5.2.3	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.AspNetCore Project homepage 🔗	2.0.2	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNetCore.Hosting.WindowsServices Project homepage 🔗	2.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNetCore.Mvc Project homepage 🔗	2.0.3	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.AspNetCore.Server.HttpSys Project homepage 🔗	2.0.3	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Bcl.AsyncInterfaces Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration.Abstractions Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration.Binder Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration.FileExtensions Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration.Json Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Configuration.UserSecrets Project homepage 🔗	2.0.1	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Extensions.FileProviders.Abstractions Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.FileProviders.Physical Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.FileSystemGlobbing Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Extensions.Logging.TraceSource Project homepage 🔗	2.0.1	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Extensions.Primitives	5.0.0	Copyright Microsoft Corporation	

Name	Version	Notice / Terms	Δ
Project homepage 🔗		Licensed under terms of MIT License 🔗	
Microsoft.Graph Project homepage 🔗	3.21.0	Copyright Microsoft Corporation Licensed under terms of License Info 🔗	
Microsoft.Graph.Core Project homepage 🔗	1.23.0	Copyright Microsoft Corporation Licensed under terms of License Info 🔗	
Microsoft.Identity.Client Project homepage 🔗	4.24.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Microsoft.Net.Http Project homepage 🔗	2.2.29	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.Owin Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Cors Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Diagnostics Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Host.HttpListener Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Hosting Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Security Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Owin.Security.Cookies Project homepage 🔗	4.1.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.ReportingServices.ReportViewerControl .Winforms Project homepage 🔗	140.340.80	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.SqlServer.SqlManagementObjects Project homepage 🔗	150.18118.0	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
Microsoft.VisualStudio.Web.CodeGeneration.Design Project homepage 🔗	2.0.3	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Microsoft.Web.Administration Project homepage 🔗	7.0.0	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
MimeKit Project homepage 🔗	2.10.1	Copyright .NET Foundation Licensed under terms of MIT License 🔗	
NHibernate Project homepage 🔗	1.2.1.4001	Copyright not listed Licensed under terms of LGPLv2 🔗	Y
Newtonsoft.Json Project homepage 🔗	6.0.4 11.0.2 12.0.3	Copyright James Newton-King Licensed under terms of MIT License 🔗	
OpenSSL Project homepage 🔗	1.1.1j	Copyright OpenSSL Project Licensed under terms of OpenSSL/SSLeay 🔗	
Owin Project homepage 🔗	1.0.0	Copyright Louis DeJardin / Chris Ross Licensed under terms of Apache 2.0 🔗	
PCLCrypto Project homepage 🔗	2.0.147	Copyright Andrew Arnott Licensed under terms of Microsoft License 🔗	
PInvoke.* Project homepage 🔗	0.7.78	Copyright .NET Foundation Licensed under terms of MIT License 🔗	
Plugin.SimpleLogger Project homepage 🔗	1.1.1	Copyright Jiri Matejka. Licensed under terms of Apache 2.0 🔗	
PJSIP Project homepage 🔗	2.3	Copyright Benny Prijono / Teluu Inc. Licensed under terms of GPLv2 🔗	Y

Name	Version	Notice / Terms	Δ
Portable.BouncyCastle Project homepage 🔗	1.8.9	Copyright Legion of the Bouncy Castle Inc. Licensed under terms of MIT License 🔗	
RestSharp Project homepage 🔗	106.11.4	Copyright John Sheehan a.o. Licensed under terms of Apache 2.0 🔗	
SharpZipLib Project homepage 🔗	1.2.0	Copyright SharpZipLib Contributors Licensed under terms of MIT License 🔗	
Sofia SIP Stack Project homepage 🔗	1.12.11	Copyright Nokia Corporation Licensed under terms of LGPL 🔗	Y
SslCertBinding.Net Project homepage 🔗	1.0.2	Copyright Serghei Gorodetki Licensed under terms of MIT License 🔗	
System.Buffers Project homepage 🔗	4.5.1	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Diagnostics.Diagnosticsource Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Memory Project homepage 🔗	4.5.4	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Numerics.Vertors Project homepage 🔗	4.5.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Runtime.CompilerServices.Unsafe Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Text.Encodings.Web Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Text.Json Project homepage 🔗	5.0.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.Threading.Tasks.Extensions Project homepage 🔗	4.5.4	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
System.ValueTuple Project homepage 🔗	4.5.0	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Unicode.net Project homepage 🔗	0.1.2	Copyright NeoSmart Technologies Licensed under terms of MIT License 🔗	Y
Unified Communications Managed API	5.0	Copyright Microsoft Licensed under terms of Microsoft License	
Validation Project homepage 🔗	2.4.22	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	
WindowsAPICodePack-Core Project homepage 🔗	1.1.2	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	Y
WindowsAPICodePack-Shell Project homepage 🔗	1.1.1	Copyright Microsoft Corporation Licensed under terms of Microsoft License 🔗	Y
Xamarin.Android.Arch.* Project homepage 🔗	1.1.1.3	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Xamarin.Android.Auth Project homepage 🔗	1.7.0	Copyright Microsoft Corporation Licensed under terms of Apache 2.0 🔗	
Xamarin.Android.Support.* Project homepage 🔗	28.0.0.3	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
Xamarin.Forms Project homepage 🔗	4.8.0.1687	Copyright Microsoft Corporation Licensed under terms of MIT License 🔗	
ZedGraph Project homepage 🔗	5.1.5	Copyright John Champion Licensed under terms of LGPLv2 🔗	Y

21. Appendix K – EXCHANGE INTEGRATION

BCT can be integrated with Microsoft Exchange for the following functionality:

- Users' calendar Free/Busy information and working hours retrieved from Exchange Server.
- User calendar popup information for operators and agents on incoming calls (or on demand).
- Operator and agent access to open a shared calendar from a user in Outlook.

Required:

- ✓ BCT license: Employee-Outlook Calendar Integration (on/off)
- ✓ For Office 365 Exchange online (using OAuth2)
  Use *https://portal.azure.com* to configure application permissions, tenant-id, client-id and client-secret for Office 365 Exchange Online. See 21.4 Configure your Office 365 Exchange online.
- ✓ Microsoft Exchange Server (for supported Exchange versions see BCT Boundary Specification)
  - Exchange Web Service (EWS) URL, typically
    https://<exchangeservername>/EWS/Exchange.asmx
    For Office 365 (Exchange Online) you can use
    https://outlook.office365.com/EWS/Exchange.asmx
    Note that <exchangeservername> must match the certificate's subject name, see 21.1 Exchange Certificate
  - Windows credentials for NT authentication
    - User Name
      Enter the user account name (e.g. 'ServiceUser') or User Principal Name (UPN) (e.g. 'ServiceUser@ucslab.local')
    - Password
      The password of this user
    - Domain
      Enter the NetBIOS domain name (e.g. UCSLAB) or leave empty when a UPN was entered in the User Name field
  - Internet Proxy Settings
    See 32 Appendix V – Exchange and Social Media Proxy Settings.
  - The Exchange certificate must be accepted by the BCT Server.
    See 21.1 Exchange Certificate.
- ✓ Exchange privileges
  See 21.2.1 Configuring calendar permission on the Exchange Server.

To configure the Exchange Server, go to System Settings, click the Miscellaneous tab and locate the "Exchange Server for Calendar Integration" field. See 8.1.12 Miscellaneous for more details.

21.1. Exchange Certificate

This section is not relevant for Office 365 Exchange online using OAuth2.
By default the Exchange Web Service is configured to communicate through a secure communication protocol (HTTPS). A prerequisite for calendar popup functionality is that the SSL certificate used for the Exchange server must be accepted by the BCT server. If the authenticity of the certificate cannot be validated, then the system cannot guarantee the communication is protected against threats like eavesdropping; therefore the connection will not be accepted.

If the certificate was issued and/or signed by a trusted certificate authority (e.g. Verisign, Thawte, Microsoft, etc.) then no further action is required.

If the certificate is issued by an unknown certificate authority, is a test certificate or is a self-created certificate, then further action is required. Before continuing, make sure that you trust this certificate and that this certificate has not yet expired.

On the Exchange Server:

1. Export the certificate file.

   In Internet Information Services (IIS) Manager, select the certificate that is used for the HTTPS connection and export the certificate to a p7b file:

   Server Certificates ->Select the certificate->View->Details->Copy to File

   Note: *Do not export the private key.*

On the Business ConneCT server:

1. On the Business ConneCT server go to Start->Run and enter “mmc.exe”
2. Select File->Add/Remove Snap-in->Add and select Certificates
3. Select Computer account and press **Next**
4. Select Local computer and press Finish. Press Close and then **OK**
5. Go to Certificates (Local Computer) and highlight Trusted Root Certification Authorities
6. Select Action->All Tasks->Import
7. Browse to the p7b file and select it. Press **Next**
8. Verify that the certificate store Trusted Root Certification Authorities is selected, press **Next**
9. Press Finish to import the certificate

The system does not accept a certificate when the host name part in the URL does not match the certificate’s Subject or the Subject Alternative Name (SAN).

To view the certificate’s Subject and the SAN:

1. On the Exchange Server, in IIS, select the certificate that is used for the HTTPS connection.
   - Server Certificates ->Select the certificate->View->Details-> Show <All>
2. Search for field Subject and Subject Alternative Name (optional).
   If for example the Subject shows ‘CN = EXCHMAIL2’ then the URL must be composed as follows: https://EXCHMAIL2/...

21.2. Exchange Privileges

By default one user can’t see or access another user’s calendar except for the basic free/busy time information. To access another user’s calendar information the user must have the appropriate access right(s). There are different methods to configure the access rights, server side or client side. Server side is used in scenarios where you need to configure the Exchange’s mailbox folder permissions for a large group of users. Client side is used for fine tuning the permissions to each individual’s preference.

All calendar integration features use the so-called Delegate Access to retrieve the calendar information. Each feature however needs a minimum level of access permission:

User's calendar Free/Busy information and working hours retrieve from Exchange Server (see chapter 9.1.2.4 Configure Microsoft Outlook (calendar) integration)

- AvailabilityOnly (= Free/Busy time only)

User calendar popup information for operators and agents on incoming calls (or on demand)

- AvailabilityOnly (= Free/Busy time only) *or*
- LimitedDetails (= Free/Busy time, subject, location)

Operator and agent access to open a shared calendar from a user in Outlook.

- Reviewer (= Full details)

21.2.1. Configuring calendar permission on the Exchange Server

To change the delegate access directly in Exchange, use the Exchange Management Shell.
In "Start->Programs->Microsoft Exchange Server" select "Exchange Management Shell"

In the PowerShell examples below the values enclosed in angle brackets should be replaced by the real value. For example replace "<User1>" by an identity name like "Bethany.Baker@domain.local".

Operator and agent access to open a shared calendar from a user in Outlook
Assign Reviewer access to the operator or agent user (For F4 functionality of Operator/Agent)

- <DelegatedUser> = the identity of the operator or agent
- <User1> = identity of a user, for example an employee's userPrincipalName
- <AccessRight> = Reviewer

Note: the <AccessRight> must be assigned to every operator and agent that uses the functionality

User calendar popup information for operators and agents on incoming calls (or on demand)
Assign AvailabilityOnly or LimitedDetails to the service user (For F5 functionality of Operator/Agent)

- <DelegatedUser> = the service user
- <User1> = identity of a user, for example an employee's userPrincipalName
- <AccessRight> = AvailabilityOnly or LimitedDetails

Note*: The <DelegatedUser> needs to have an email account.*

Assigning mailbox folder permission

To assign delegate access, enter the following command.

```
Add-MailboxFolderPermission -Identity <user1>:\Calendar -User: <DelegatedUser>
-AccessRights <AccessRight>
```

Note: *The part "Calendar" is language pack dependent. Can also be "Kalendar" or "Agenda".*

To modify a delegate access, enter the following command.

```
Set-MailboxFolderPermission -Identity <user1>:\Calendar -User: <DelegatedUser>
-AccessRights <AccessRight>
```

For more information see: https://technet.microsoft.com/en-us/library/dn641230.aspx

Assigning mailbox folder permission to multiple users

The MailboxfolderPemission cmdlets can only add or change the delegate access for a single user. PowerShell however allows you to run the command for a list of users. Which users to apply to and where the list comes from is up to you.

Here are two random examples: users from an OU or users from a text file.

```
Get-User -OrganizationalUnit "OU="Users,DC=YourDomain,DC=com" |
foreach { Add-MailboxFolderPermission -identity "$($_.UserPrincipalName):\Calendar"
-User <DelegatedUser> -AccessRights <AccessRight>}
```

```
Get-Content "C:\Users\MyCompanyUsers.txt" | foreach {Add-MailboxFolderPermission
-identity "$($_):\Calendar" -User <DelegatedUser> -AccessRights <AccessRight>}
```

21.2.2. Modifying calendar permission with Outlook or OWA

Every user can add, change or remove the calendar permissions in their own Outlook or OWA.

To manage these permissions in Outlook, go to Calendar and press the Calendar Permissions button. Here users can change or remove the permission that were assigned to the operator and/or agent and/or the service user.

To manage these permissions in OWA (Outlook Web Access) go to Calendar, My Calendars, right click on Calendar and select Permissions.

21.3. Test your Exchange Configuration Settings

This section is not relevant for Office 365 Exchange online using OAuth2.

After configuring the Exchange settings the Business ConneCT health system might trigger alarms (see chapter 11.4.3.32 Exchange Web Service connection Alarm [6112]) when the settings are not accepted. It might be hard to determine the actual problem based on the alarm description. An easier way to verify the configuration settings is by using Internet Explorer/Edge browser.

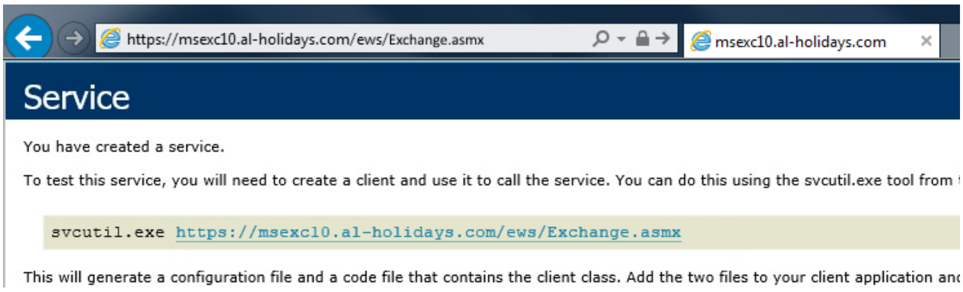
To test your Exchange configuration settings with Internet Explorer:

1. Launch Internet Explorer

2. In the Link address enter your Exchange Web Service (EWS) URL (for example *https://msexch10.al-holidays.com/EWS/Exchange.asmx*) and press **Enter**.

3. If the Exchange Web Service requires credentials, enter the credentials in the login dialog.

4. If the settings are correct you will see the following output:



Service

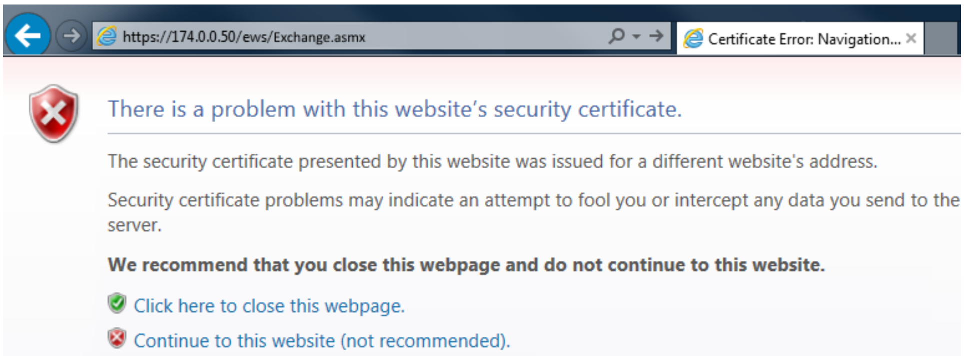
You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the svcutil.exe tool from

```
svcutil.exe https://msexc10.al-holidays.com/ews/Exchange.asmx
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application an

However, when the certificate is not installed correctly or URL doesn't match the certificate's Subject Name then you will see the following:


https://174.0.0.50/ews/Exchange.asmx
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

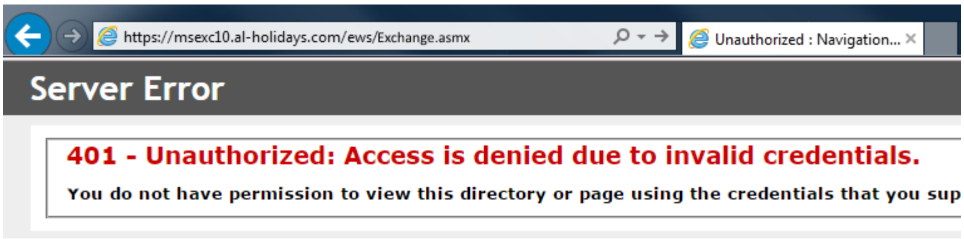
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

In this case the host name from the URL (174.0.0.50) does not match the certificate's Subject Name of Subject Alternative Name: msex10.al-holidays.com. Changing the URL to https://msexc10.al-holidays.com/ews/Exchange.asmx would resolve the issue.

When the credentials are incorrect then you will see a page similar to this:


https://msexc10.al-holidays.com/ews/Exchange.asmx
Unauthorized : Navigation...

Server Error

401 - Unauthorized: Access is denied due to invalid credentials.

You do not have permission to view this directory or page using the credentials that you sup

Try again using the correct credentials or ask your IT department to allow your account access to the Exchange server.

21.4. Configure your Office 365 Exchange online (with OAuth2) for Calendar integration

- Login to your Azure account (Home) and enter "App registrations".

- If there are already applications registered, one of the applications can be used for calendar integration, if none are present or it is needed to create an additional application: create a new application first.

- Click on the selected application
  Note down or copy the Tenant ID (Directory ID) for entry in System Settings.
  Note down or copy the Client ID (Application ID) for entry in System Settings.

- If a new Client Secret is to be used, click on "Certificates & secrets" and select "New client secret". Give a description and select the expiration and click "Add".
  Note down or copy the generated Value of the secret (for entry in System Settings) as it will only be shown once, leaving this page will not reveal the value again.

- Click on "API permissions"

  - If "Office 365 Exchange Online" is not visible, it has to be made visible first. Click on "Add permission" and search whether Office 365 Exchange Online is visible as a tile in the list. If visible click it and continue with the next bullet item,

otherwise: Click on “Manifest” and locate "requiredResourceAccess" in the shown data.
If the value of "requiredResourceAccess" is empty (i.e. only contains “[]”), copy the below JSon element (shown in grey), copy the text from opening curly bracket “{“uptil/including the closing curly bracket “}” and paste it between the square brackets “[]” in "requiredResourceAccess":

JSon element to be inserted:

```
{"resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
 "resourceAccess": [
   {"id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
    "type": "Role"
   } ]
 }
```

and click “Save”.
If the value of "requiredResourceAccess" is not empty between the square brackets, then copy the above JSon element (shown in grey), paste it in "requiredResourceAccess" just after the opening square bracket “[” and add a comma after the closing curly bracket “}” of the inserted JSon element and click “Save”, now continue with the next bullet item.
For additional information see https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth

- ○ In “API permissions” the “Office 365 Exchange Online” row should now be visible. Verify that “full_access_as_app” is already present as permission.
Click on “Office 365 Exchange Online” to add extra permissions then click on tile “Application permissions” and select Calendars.Read and Calendars.Read.All and click “Update permissions”.
Afterwards click “Grant admin consent for …” and select Yes to confirm the selected permissions.

- After configuring the settings the Business ConneCT health system might trigger alarms (see chapter 11.4.3.32 Exchange Web Service connection Alarm [6112]) when the settings are not correct. Verify in system settings whether the Tenant-Id, Client-id and Client-secret are correctly copied from the data present in Azure.

22. Appendix L – HOW TO LIMIT PUBLIC ACCESS TO BCT WEB PAGES AND WEB APPLICATIONS

When a customer wants some BCT functionality be available from outside the company network, the BCT Server is placed in the DMZ. By default all BCT web pages and folders are then publicly accessible from the internet. Some of the BCT web pages are redirected via Central Authentication (CA) so the user must login first, but others are directly accessible.

These pages are not required to be available outside the network (segment) of the BCT Server and clients, and should be protected against unauthorized external access. Only when the customer wants to be able to use particular functionality outside the company network (from the internet), some of these pages must be made available for external access.

For general information and guidelines about addressing and managing network security risks, see the whitepaper: “Business ConneCT Mobile Client Network Security”. This document describes how to (de)couple IIS (from) to the internet.

To limit the access to the BCT web pages, IIS has a way to restrict all but a certain subset of IP addresses to have access to IIS pages:

1. Open the Web Server (IIS).
2. Verify that the *IP and Domain Restrictions Role* has been installed on the server
3. Double-click the **IPv4 Address and Domain Restrictions** icon.
4. Click on the **Edit Feature Settings** link (on the right side of the window)
5. Now you will see the **Edit and Domain Restrictions Settings** dialog box
6. Select ‘Deny’ and click **OK**. Anyone accessing the site will now get a *403 – Forbidden* error.
7. To let some IP addresses in, you can add a single address or range of addresses specifically.

   If you want to let only one PC into the server, you have to add an Allow Restriction Rule for its specific IP address.

   If you need a less specific range, you have to add an Allow Restriction Rule for an address range, for example your internal office network addresses.

   Let’s assume that they are in the 10.160.30.xxx range. Then you have to specify:
   IPv4 address range: 10.160.30.0
   Mask: 255.255.255.0
   This will be the entire class ‘C’ range (255.255.255.0) of the 10.160.30.0 subnet.

   Note: *XML Clients load several web applications for correct operation. This is done by sending HTTP requests, which use 'localhost'. To ensure that the XML Clients start properly, you need to add an Allow Restriction Rule for 'localhost'.*

8. To provide access for external clients, you need to specify their external IP addresses. and for each IP-address add an Allow Restriction Rule. This assumes that the external address is

static – if it's dynamic and it changes, then you will have to Delete and Re-add the rule with the new IP address before they will have access again.

9. Now only the internal network and anyone on the client's network have access to the site – for the rest of the internet, it is a 403 error.

23. Appendix M – ESSENTIAL EMPLOYEE CLIENT INSTALLATION AND CONFIGURATION

This appendix contains additional information on installation and configuration of BCT and/or iS3000/SIP@Net, with respect to specific functionality, introduced for ‘Essential Employee Client’.

It only describes **changes** and/or **additions** compared to the standard BCT Installation.

23.1. System requirements

23.1.1. PBX requirements

BCT, with respect to the BCT Essential Employee Client, is only supported in combination with SIP@NET 5.1 or higher, SV8100/SV9100, SV8300/SV9300 and SV8500/SV9500.

23.2. SIP@NET configuration

In addition to the information given in the BCT Installation Guide following SIP@Net related configuration aspects are relevant.

23.2.1. Boundaries and options

BCT requires specific values for boundaries and options, given in this section.

Use the **DIMDAT** command to read the values. If necessary, correct them; do a retrieve, make changes, restore the projecting files into the system and re-project the system. The Second Line Maintenance Manual describes how to do this.

Boundaries

- BOUND218: MAX NUMBER OF LONG FACILITY DESTINATIONS
  Default = 50; Max= 1000. Defines the maximum number of external call forwarding destinations that can be configured in a system. Please change this number by taking into account the number of BCT Essential Employee users.

Options

- LOSYSOP207: MOVE TO ORIGINAL CIRCUIT ON DEACTIVATE SMA
  Default = false; In case the CSTA application deactivates SMA or the SMA user dials the 'Deactivate DNR' prefix (Result ID 51) the DNR is made hardware less. When this option is set to “TRUE”, the previous EHWA of the DNR is stored and on deactivation of the SMA the DNR is moved back to this EHWA again. When system option 190 is set this will be journalled as well. (note that also Desksharing (FCM 57) is required). When this option is set to “FALSE”, the DNR is not moved back.

23.2.2. Facility Class Marks

For a BCT Essential Employee user to access following functionality, it is required to assign the following facility classmarks (FCM) to the user’s extension:

- Follow Me/Call Forwarding
  Assign FCM 7

- **SMA**
  Assign FCM 75

- DND
  Assign FCM 25

23.3. SV8100/SV9100 configuration

The SV8100/SV9100 should NOT be configured to support internal and external Call Forwarding's, as it does not support SPLIT Call Forwarding.

23.4. SV8300/SV9300 configuration

The SV8300/SV9300 should NOT be configured to support internal and external Call Forwarding's, as it does not support SPLIT Call Forwarding.

23.5. SV8500/SV9500 configuration

The SV8500/SV9500 should NOT be configured to support internal and external Call Forwarding's, as it does not support SPLIT Call Forwarding.

23.6. BCT Server configuration

23.6.1. Manually create a user

In addition to the information in 8.5.10 Manually create a BCT user, for BCT Essential Employee users the following actions are required:

1. Assign role 'Essential Employee'

2. Make sure there is a free 'Essential Employee' license available (this is a user-based license, statically assigned)

23.7. BCT Essential Employee Client installation and configuration

23.7.1. Installation

The BCT Essential Employee Client application is part of the default BCT Server installation. When the BCT server installation is finished then all the relevant components for the BCT Essential Employee Client application are installed and ready to use.

23.7.2. Configuration

The BCT Essential Employee Client can be accessed via a web browser on a PC. For the BCT Essential Employee Client to work correctly, it is required to enable the following options in the web browser:

- JavaScript support
- Cookies support

23.7.3. How to access BCT Essential Employee Client

The internet address (URL) to get access to the BCT Essential Employee Client is in the following format:

http://<FQDN-BCT-Server-name>/EssentialClient

or

http://<FQDN-BCT-Server-name>/E

After entering this URL the BCT Essential Employee Client login page will be displayed, via which a user can enter his/her credentials and gain access to the functionality offered by the BCT Essential Employee client.

23.7.4. BCT Essential Employee troubleshooting

Problem: After login I get an error message 'Sign in failed. You do not have the proper rights'.

Solution: You entered incorrect user credentials or you do not have the role 'Essential Employee' assigned.

Problem: After each page access I have to login again.

Solution: Your browser does not support cookies, or they have been prohibited. Change your browser settings to allow cookies.

Problem: I only get a login screen.

Solution: Your browser does not support cookies, or they have been prohibited. Change your browser settings to allow cookies.

Problem: I cannot set/reset my call forwarding settings.

Solution: In case your extension resides on a Sip@Net PBX, your extension does not have FCM 7 assigned.

Problem: I do not have access to my SMA settings.

Solution: In case your extension resides on a SV8100/SV9100, SV8300/SV9300 or SV8500/SV9500 this is correct. Otherwise, in case your extension resides on a Sip@Net PBX, your extension does not have FCM 75 assigned.

Problem: I do not have access to my DND settings.

Solution: In case your extension resigns on a Sip@Net PBX, your extension does not have FCM 25 assigned.

Problem: I do not have access to my ACD Group presence settings.

Solution: In case your extension resigns on a SV8100/SV9100, SV8300/SV9300 or SV8500/SV9500 this is correct, these PBX's do not support ACD groups. Else your extension is not part of an ACD Group configuration in a SIP@Net PBX.

Problem: When I deactivate my SMA setting my DNR is not moved back to my previously used extension.

Solution: Option 207 is not set correctly in SIP@Net. Please refer to 23.2.1 Boundaries and options.

24. Appendices N – BCT ON UNIVERGE 3C CONFIGURATION DETAILS

24.1. Appendix N-1 – Configure Operator Fallback for failed external calls

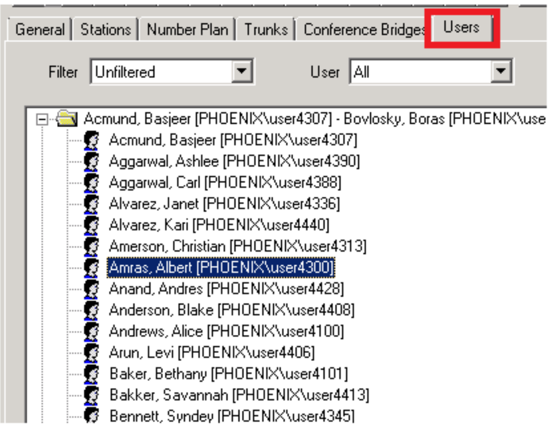
External calls that encounter a destination that is either busy, not answering or in Do Not Disturb mode can be rerouted to the operator fallback Queue (8952 in our example). Also external calls to a non-existing destination can be rerouted to the operator fallback Queue. In the UNIVERGE 3C, rerouting is accomplished by setting Call Forwarding on the stations and trunks.

24.1.1. Set Call Forwarding on individual users/extensions

If externals callers should be rerouted to the Operator if the called party is busy, not answering, or in Do Not Disturb, perform the following steps.

Note: *Forwarding is set slightly different depending on if the User is Address Centric or User Centric.*
Note: *If you have an existing UNIVERGE 3C system that has been running for some time and CF conditions and profiles have already been defined, you have to be careful not to overwrite existing profiles. Please check the schedule of existing profiles.*

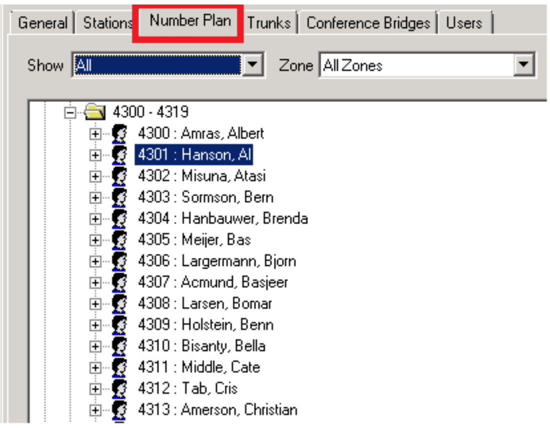
1. Open the UNIVERGE 3C Administrator and choose the Users tab for User Centric users or the Number Plan tab for Address Centric users.



Filter Unfiltered
User All

Acmund, Basjeer [PHOENIX\user4307] - Bovlosky, Boras [PHOENIX\use
Acmund, Basjeer [PHOENIX\user4307]
Aggarwal, Ashlee [PHOENIX\user4390]
Aggarwal, Carl [PHOENIX\user4388]
Alvarez, Janet [PHOENIX\user4336]
Alvarez, Kari [PHOENIX\user4440]
Amerson, Christian [PHOENIX\user4313]
Amras, Albert [PHOENIX\user4300]
Anand, Andres [PHOENIX\user4428]
Anderson, Blake [PHOENIX\user4408]
Andrews, Alice [PHOENIX\user4100]
Arun, Levi [PHOENIX\user4406]
Baker, Bethany [PHOENIX\user4101]
Bakker, Savannah [PHOENIX\user4413]
Bennett, Syndey [PHOENIX\user4345]

User Centric



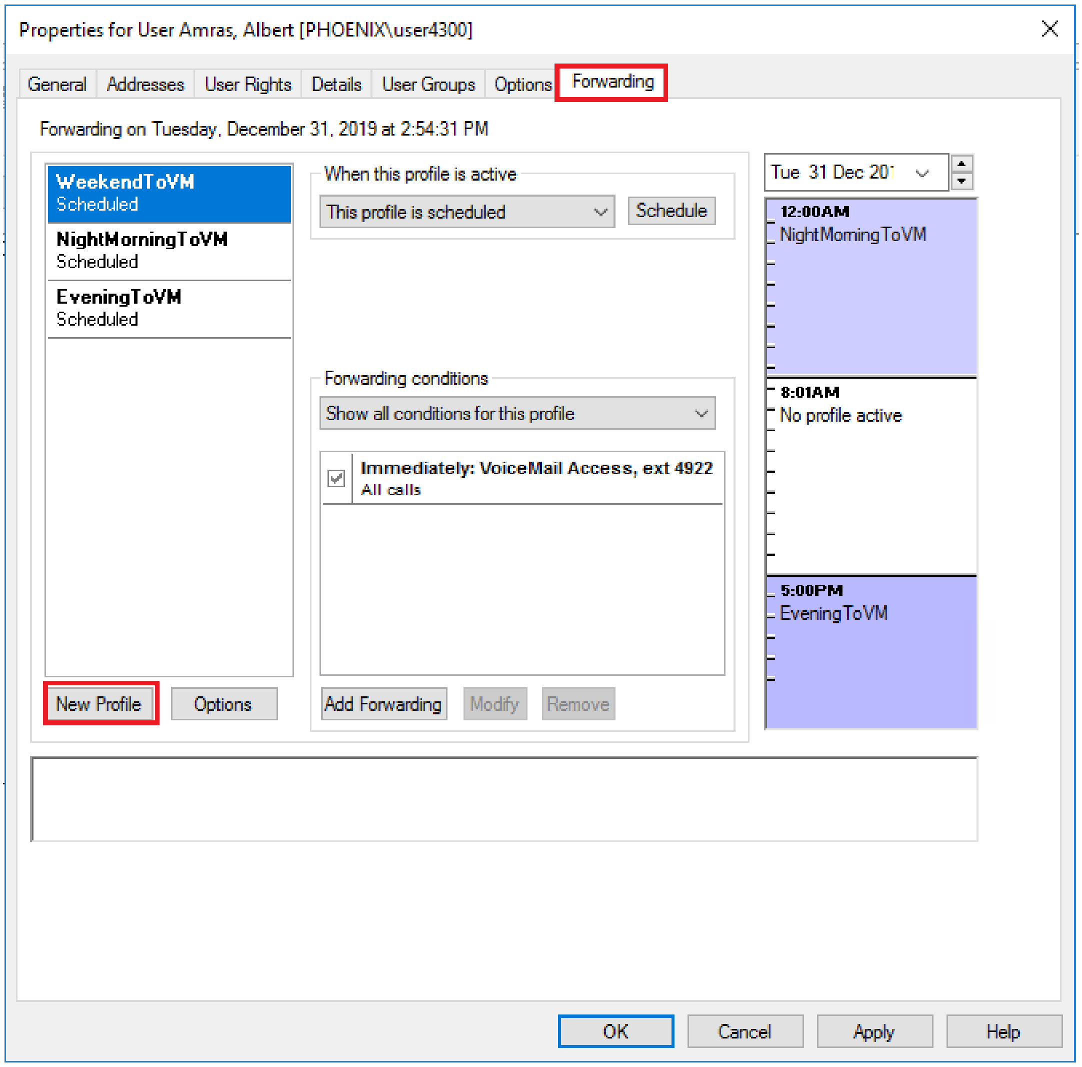
Show All
Zone All Zones

4300 - 4319
4300 : Amras, Albert
4301 : Hanson, Al
4302 : Misuna, Atasi
4303 : Sormson, Bern
4304 : Hanbauwer, Brenda
4305 : Meijer, Bas
4306 : Largermann, Bjorn
4307 : Acmund, Basjeer
4308 : Larsen, Bomar
4309 : Holstein, Benn
4310 : Bisanty, Bella
4311 : Middle, Cate
4312 : Tab, Cris
4313 : Amerson, Christian

Address Centric

2. Double-click the User the forwarding is to be set to open the User/Extension Properties window.

3. Select the Forwarding tab and click the **New Profile** button.



Properties for User Amras, Albert [PHOENIX\user4300]

Forwarding on Tuesday, December 31, 2019 at 2:54:31 PM

WeekendToVM
Scheduled

NightMorningToVM
Scheduled

EveningToVM
Scheduled

When this profile is active: This profile is scheduled

Forwarding conditions: Show all conditions for this profile

☑ **Immediately: VoiceMail Access, ext 4922**
All calls

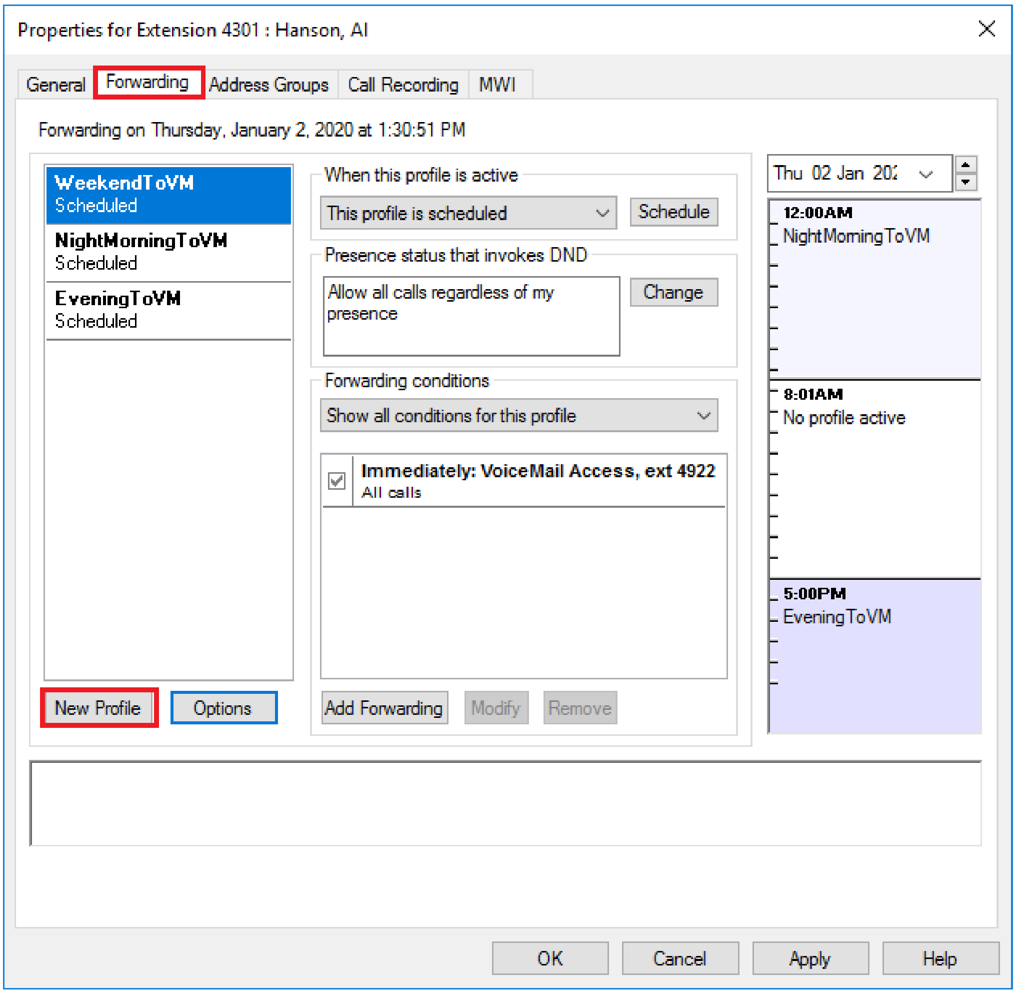
Tue 31 Dec 201

12:00AM NightMorningToVM

8:01AM No profile active

5:00PM EveningToVM

User Centric

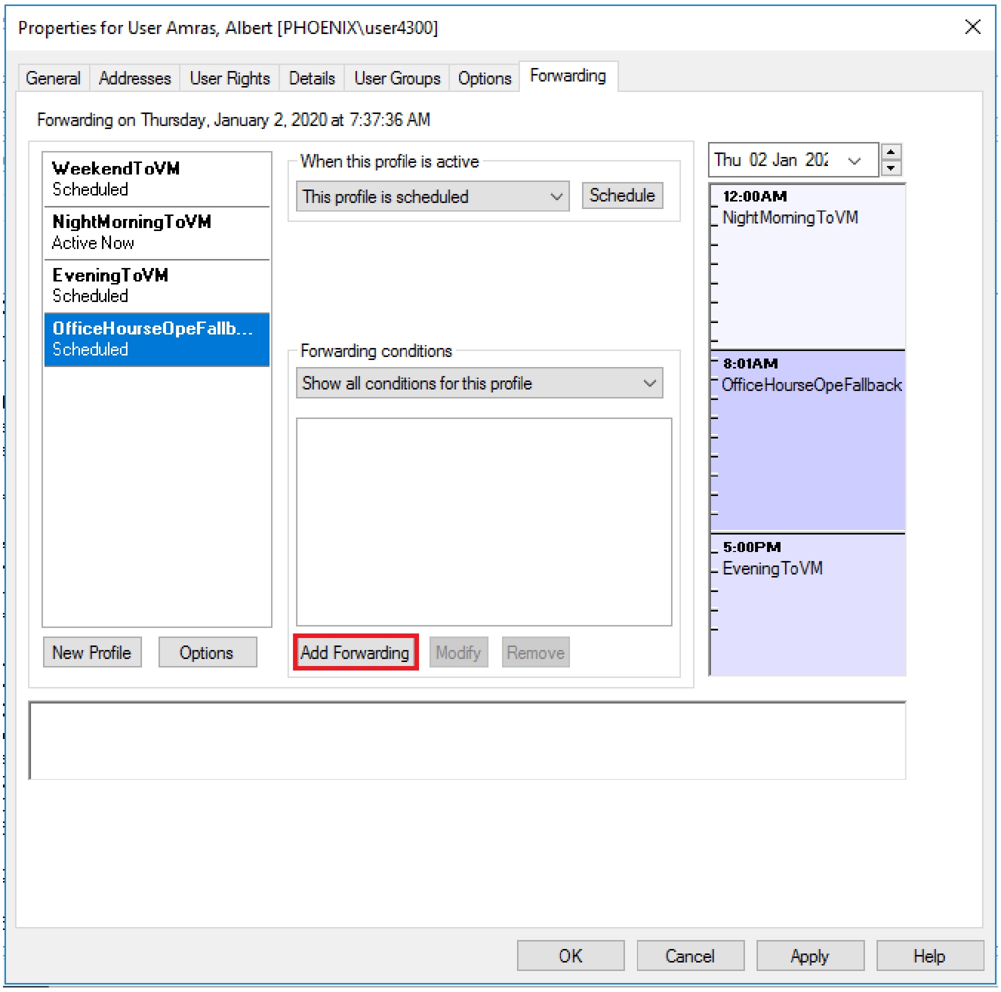

Properties for Extension 4301 : Hanson, Al
General
Forwarding
Address Groups
Call Recording
MWI
Forwarding on Thursday, January 2, 2020 at 1:30:51 PM
WeekendToVM
Scheduled
NightMorningToVM
Scheduled
EveningToVM
Scheduled
When this profile is active
This profile is scheduled
Schedule
Presence status that invokes DND
Allow all calls regardless of my presence
Change
Forwarding conditions
Show all conditions for this profile
☑ Immediately: VoiceMail Access, ext 4922
All calls
New Profile
Options
Add Forwarding
Modify
Remove
Thu 02 Jan 202
12:00AM
NightMorningToVM
8:01AM
No profile active
5:00PM
EveningToVM
OK
Cancel
Apply
Help

Address Centric

4. Type a name for the new forwarding profile then click **OK**.

5. In the Schedule window, set the Day, Start Time and End time according to the required schedule, for instance for office hours and click **OK**. Be careful not to overwrite any existing forwarding conditions, for instance forwarding to Voicemail outside office times.

6. Click the new forwarding profile to highlight it, then click the Add Forwarding button.



Forwarding on Thursday, January 2, 2020 at 7:37:36 AM

WeekendToVM – Scheduled
NightMorningToVM – Active Now
EveningToVM – Scheduled
OfficeHourseOpeFallb... – Scheduled

When this profile is active: This profile is scheduled

Forwarding conditions: Show all conditions for this profile

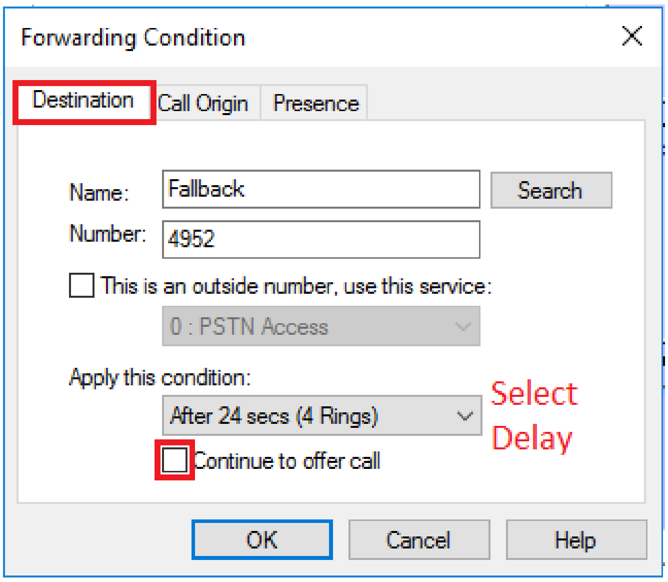
Thu 02 Jan 202

12:00AM NightMorningToVM
8:01AM OfficeHourseOpeFallback
5:00PM EveningToVM

7. Select the Destination tab in the Forwarding Condition window.

- Number: Enter the number that this User will forward to. (4952 in this example)
- Apply this condition: Use the drop-down menu to select how long to wait before following the forwarding
- Continue to offer call: **Do not check** this option!

Note: the Name is updated after Apply the changes.



Forwarding Condition

Destination | Call Origin | Presence

Name: Fallback

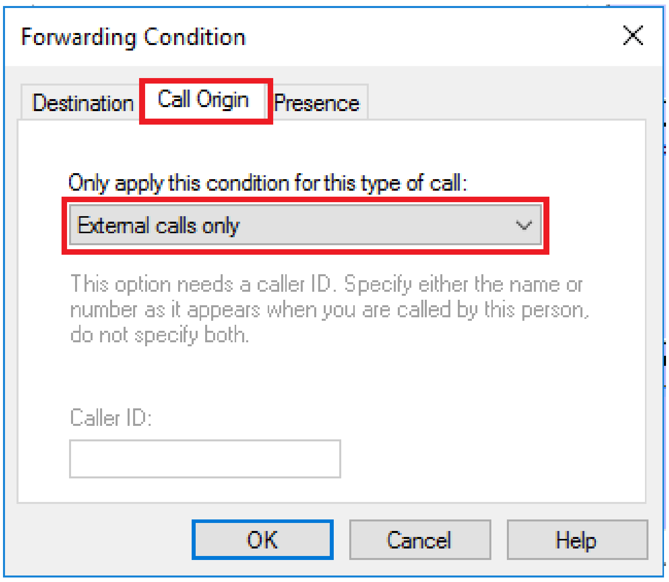
Number: 4952

☐ This is an outside number, use this service: 0 : PSTN Access

Apply this condition: After 24 secs (4 Rings)

☐ Continue to offer call

8. Select the Call Origin tab and set the condition to “External calls only” and then click **OK**.



Forwarding Condition

Destination | Call Origin | Presence

Only apply this condition for this type of call: External calls only

This option needs a caller ID. Specify either the name or number as it appears when you are called by this person, do not specify both.

Caller ID:

24.1.2. Set Call Forwarding on multiple users/extensions

CAUTION: *In this example there are no forwarding profiles and conditions already present on the system and the profile added will be the standard profile called “Forwarding Profile”. The procedure of adding bulk forwarding conditions works just fine for new installations of UNIVERGE 3C.*

However, if you have an existing UNIVERGE 3C system that has been running for some time and CF conditions and profiles have already been defined, you have to be careful using the bulk mechanism because improper use may damage existing CF conditions (including those set by individual users). We recommend backing up the PBX database before using the Bulk CF mechanism.

Alternatively, you can choose to set the CF conditions per user or per extension, but this can take quite some time in larger systems.

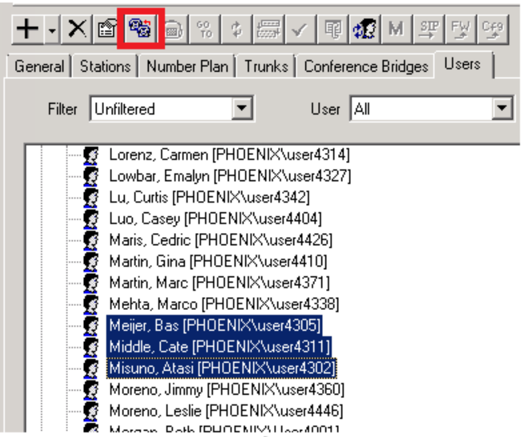
Note: *Forwarding is set slightly different depending on if the User is Address Centric or User Centric.*

1. Open the UNIVERGE 3C Administrator and choose the Users tab for User Centric users or the Number Plan tab for Address Centric users.

2. Select multiple users by first clicking on one user then, holding the Shift key down, click on another user above or below the first. All users between the two selected will also be selected.

   Note: *Multi-select using the CTRL key does not work.*

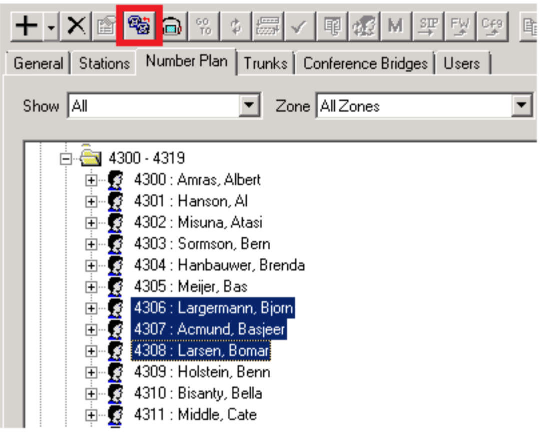
3. Click the Set Forward button to open the Set Forwarding window.



Filter: Unfiltered
User: All

Lorenz, Carmen [PHOENIX\user4314]
Lowbar, Emalyn [PHOENIX\user4327]
Lu, Curtis [PHOENIX\user4342]
Luo, Casey [PHOENIX\user4404]
Maris, Cedric [PHOENIX\user4426]
Martin, Gina [PHOENIX\user4410]
Martin, Marc [PHOENIX\user4371]
Mehta, Marco [PHOENIX\user4338]
Meijer, Bas [PHOENIX\user4305]
Middle, Cate [PHOENIX\user4311]
Misuno, Atasi [PHOENIX\user4302]
Moreno, Jimmy [PHOENIX\user4360]
Moreno, Leslie [PHOENIX\user4446]

User Centric

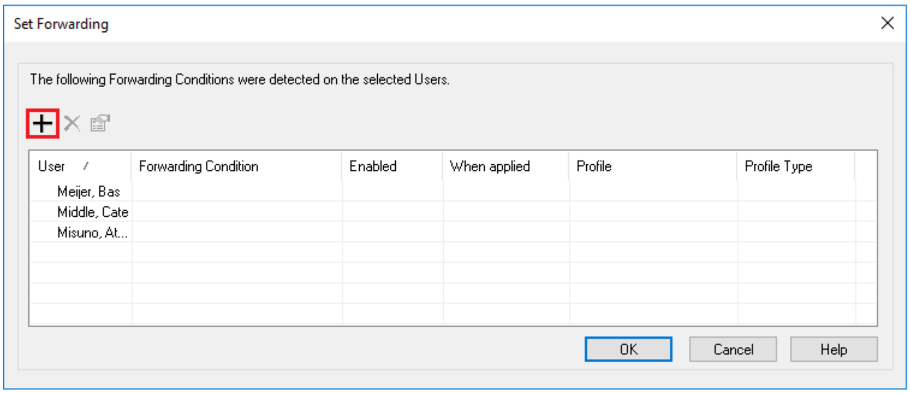


Show: All
Zone: All Zones

4300 - 4319
4300 : Amras, Albert
4301 : Hanson, Al
4302 : Misuna, Atasi
4303 : Sormson, Bern
4304 : Hanbauwer, Brenda
4305 : Meijer, Bas
4306 : Largermann, Bjorn
4307 : Acmund, Basjeer
4308 : Larsen, Bomar
4309 : Holstein, Benn
4310 : Bisanty, Bella
4311 : Middle, Cate

Address Centric

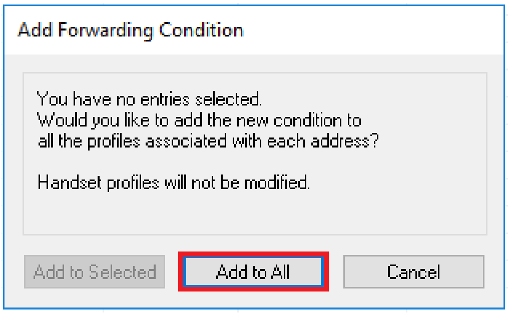
4. Click the **Add Condition** button to open the Add Forwarding Condition window.



The following Forwarding Conditions were detected on the selected Users.

User	Forwarding Condition	Enabled	When applied	Profile	Profile Type
Meijer, Bas					
Middle, Cate					
Misuno, At...					

5. Click the Add to All button. The Forwarding Condition window opens.



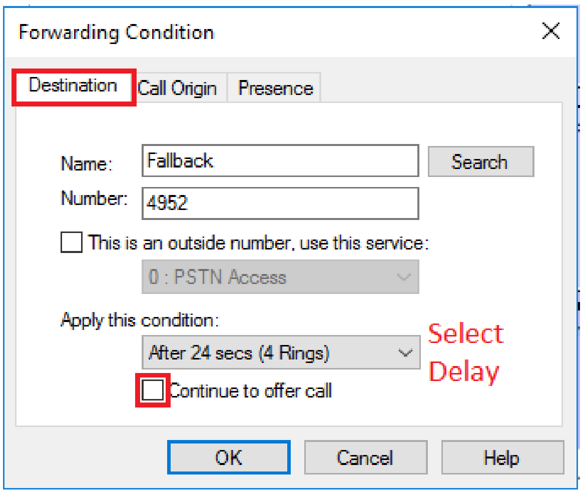
You have no entries selected.
Would you like to add the new condition to
all the profiles associated with each address?

Handset profiles will not be modified.

6. Select the Destination tab in the Forwarding Condition window.

- Number: Enter the number that this User will forward to. (4952 in this example)
- Apply this condition: Use the drop-down menu to select how long to wait before following the forwarding
- Continue to offer call: **Do not check** this option!

Note: the Name is updated after Apply the changes.



Name: Fallback

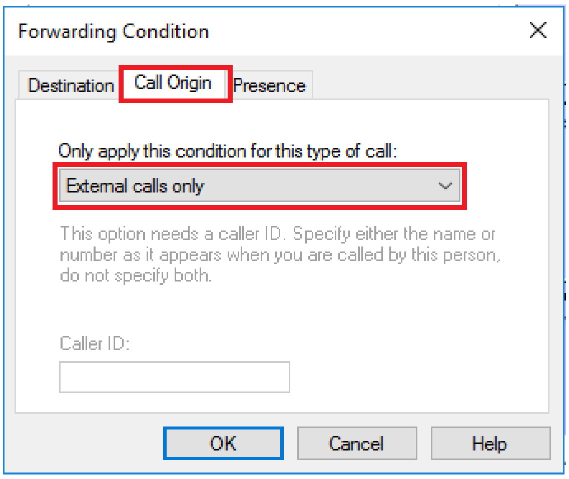
Number: 4952

□ This is an outside number, use this service: 0 : PSTN Access

Apply this condition: After 24 secs (4 Rings)

□ Continue to offer call

7. Select the Call Origin tab and set the condition to "External calls only" and then click **OK**.

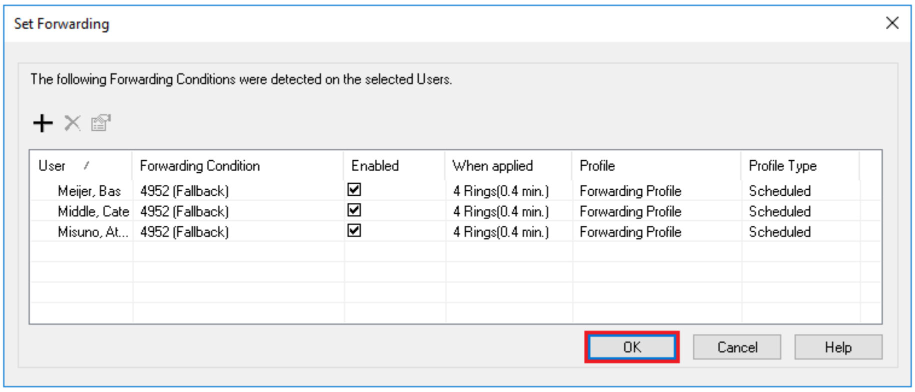


Only apply this condition for this type of call: External calls only

This option needs a caller ID. Specify either the name or number as it appears when you are called by this person, do not specify both.

Caller ID:

8. The Set Forwarding should appear similar to the image below. Click **OK** to complete setting the call forwarding.



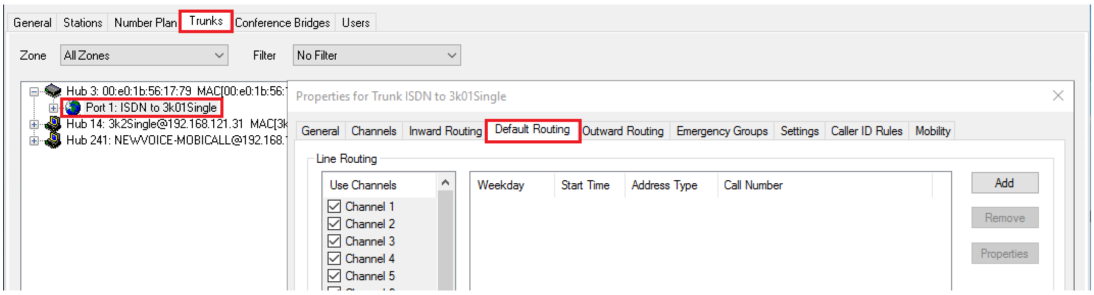
The following Forwarding Conditions were detected on the selected Users.

User /	Forwarding Condition	Enabled	When applied	Profile	Profile Type
Meijer, Bas	4952 (Fallback)	☑	4 Rings(0.4 min.)	Forwarding Profile	Scheduled
Middle, Cate	4952 (Fallback)	☑	4 Rings(0.4 min.)	Forwarding Profile	Scheduled
Misuno, At...	4952 (Fallback)	☑	4 Rings(0.4 min.)	Forwarding Profile	Scheduled

24.1.3. Configuring operator fallback for calls to non existing extension – ISDN trunks

1. Open the UNIVERGE 3C Administrator and choose the Trunks tab.

2. Expand the Hub holding the Port for the ISDN trunk. Double click the ISDN Port.



Zone: All Zones
Filter: No Filter

- Hub 3: 00:e0:1b:56:17:79 MAC[00:e0:1b:56:1
  - Port 1: ISDN to 3k01Single
- Hub 14: 3k2Single@192.168.121.31 MAC[3k
- Hub 241: NEWVOICE-MOBICALL@192.168.1

Properties for Trunk ISDN to 3k01Single

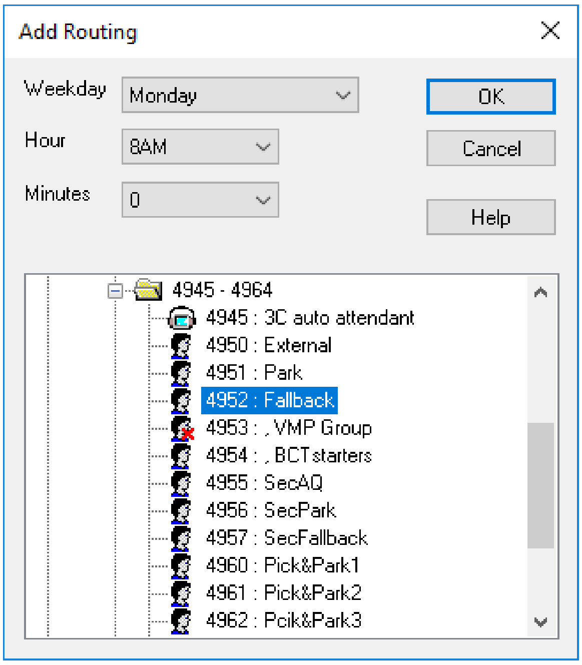
Line Routing

Use Channels
☑ Channel 1
☑ Channel 2
☑ Channel 3
☑ Channel 4
☑ Channel 5

Weekday	Start Time	Address Type	Call Number

3. In the Trunk Properties window, choose the Default Routing tab and click the **Add** button.

4. In the Add Routing window, select Sunday for Weekday, 12AM for Hour, and 0 for Minutes (midnight). Then select the Operator Fallback number (4952 in this example) and click **OK**.

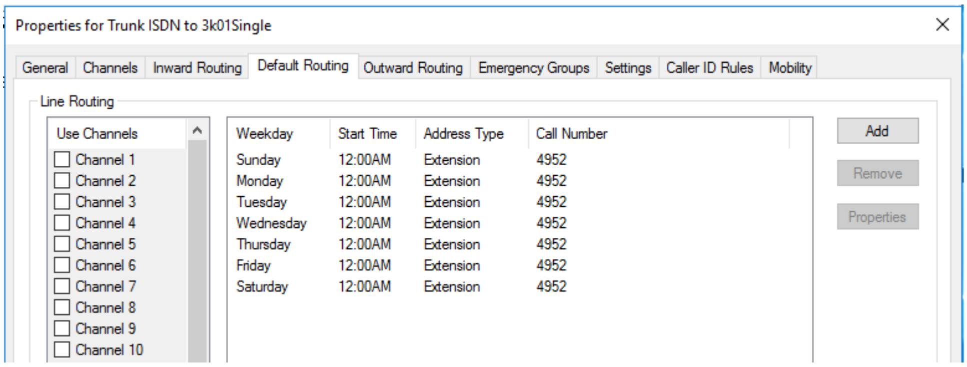


Add Routing

Weekday: Monday
Hour: 8AM
Minutes: 0

- 4945 - 4964
  - 4945 : 3C auto attendant
  - 4950 : External
  - 4951 : Park
  - 4952 : Fallback
  - 4953 : , VMP Group
  - 4954 : , BCT starters
  - 4955 : SecAQ
  - 4956 : SecPark
  - 4957 : SecFallback
  - 4960 : Pick&Park1
  - 4961 : Pick&Park2
  - 4962 : Pcik&Park3

5. Repeat step 4 for each day of the week so that the Trunk Properties window displays as shown below. Click **OK** to complete setting Call Forwarding.



Properties for Trunk ISDN to 3k01Single

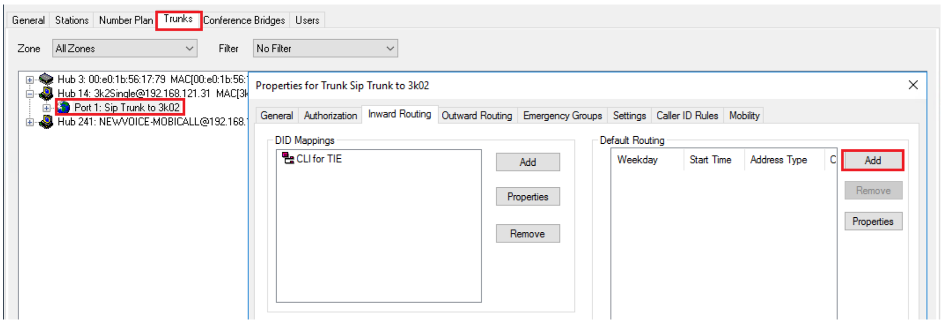
Line Routing

Weekday	Start Time	Address Type	Call Number
Sunday	12:00AM	Extension	4952
Monday	12:00AM	Extension	4952
Tuesday	12:00AM	Extension	4952
Wednesday	12:00AM	Extension	4952
Thursday	12:00AM	Extension	4952
Friday	12:00AM	Extension	4952
Saturday	12:00AM	Extension	4952

24.1.4. Configuring operator fallback for calls to non existing extensions – SIP trunks

1. Open the UNIVERGE 3C Administrator and choose the Trunks tab.

2. Expand the Hub holding the Port for the SIP trunk. Double click the SIP Port.



Zone: All Zones Filter: No Filter

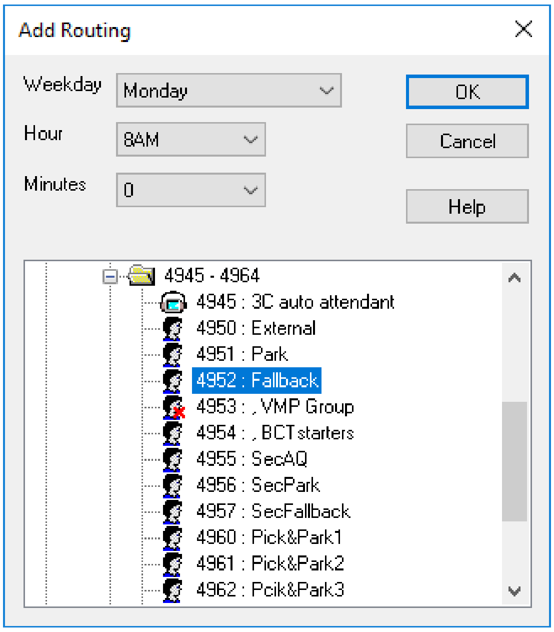
Hub 3: 00:e0:1b:56:17:79 MAC[00:e0:1b:56:
Hub 14: 3k2Single@192.168.121.31 MAC[3k
Port 1: Sip Trunk to 3k02
Hub 241: NEWVOICE-MOBICALL@192.168.

Properties for Trunk Sip Trunk to 3k02

DID Mappings: CLI for TIE

3. In the Trunk Properties window, choose the Inward Routing tab and click the Add (Default Routing) button.

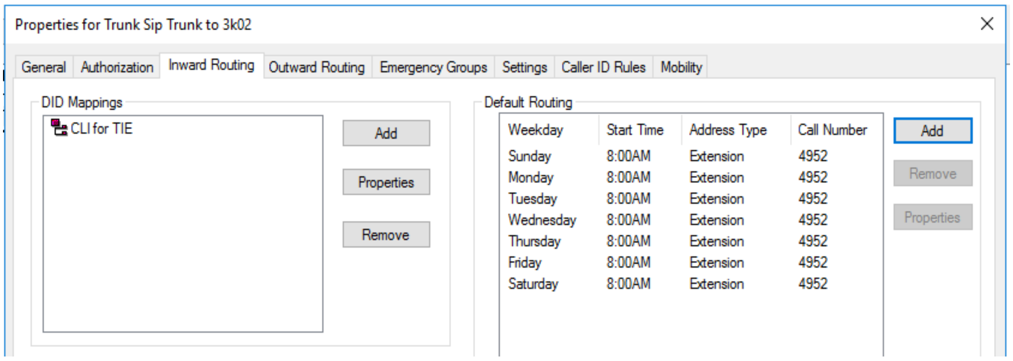
4. In the Add Routing window, select Sunday for Weekday, 12AM for Hour, and 0 for Minutes (midnight). Then select the Operator Fallback number (4952 in this example) and click OK.



Weekday: Monday
Hour: 8AM
Minutes: 0

4945 - 4964
4945 : 3C auto attendant
4950 : External
4951 : Park
4952 : Fallback
4953 : , VMP Group
4954 : , BCT starters
4955 : SecAQ
4956 : SecPark
4957 : SecFallback
4960 : Pick&Park1
4961 : Pick&Park2
4962 : Pcik&Park3

5. Repeat step 4 for each day of the week so that the Trunk Properties – Default Routing window displays as shown below. Click **OK** to complete Call Forwarding.



CLI for TIE

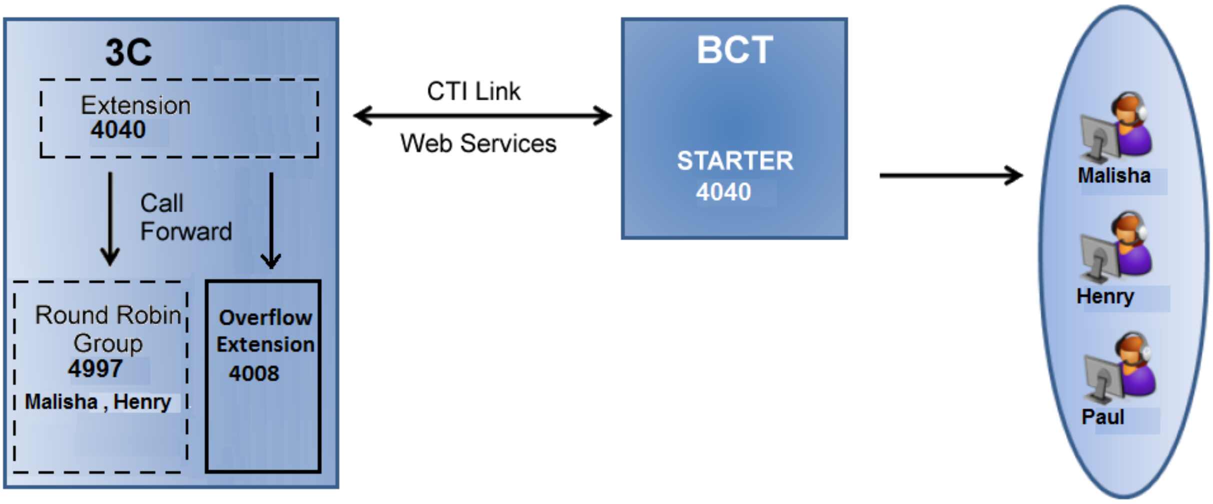
Weekday	Start Time	Address Type	Call Number
Sunday	8:00AM	Extension	4952
Monday	8:00AM	Extension	4952
Tuesday	8:00AM	Extension	4952
Wednesday	8:00AM	Extension	4952
Thursday	8:00AM	Extension	4952
Friday	8:00AM	Extension	4952
Saturday	8:00AM	Extension	4952

24.2. Appendix N-2 – Configure BCT Failover to UNIVERGE 3C

Ideally there should always be a CTI connection between BCT server and the UNIVERGE 3C system, however in real live situation network connections may be disrupted to the UNIVERGE 3C system or the BCT server HW could fail. In such cases a failover scenario is needed so that operator calls and/or contact center calls can be handled by the UNIVERGE 3C system. Of course this functionality is limited compared to BCT, but at least calls are not lost.

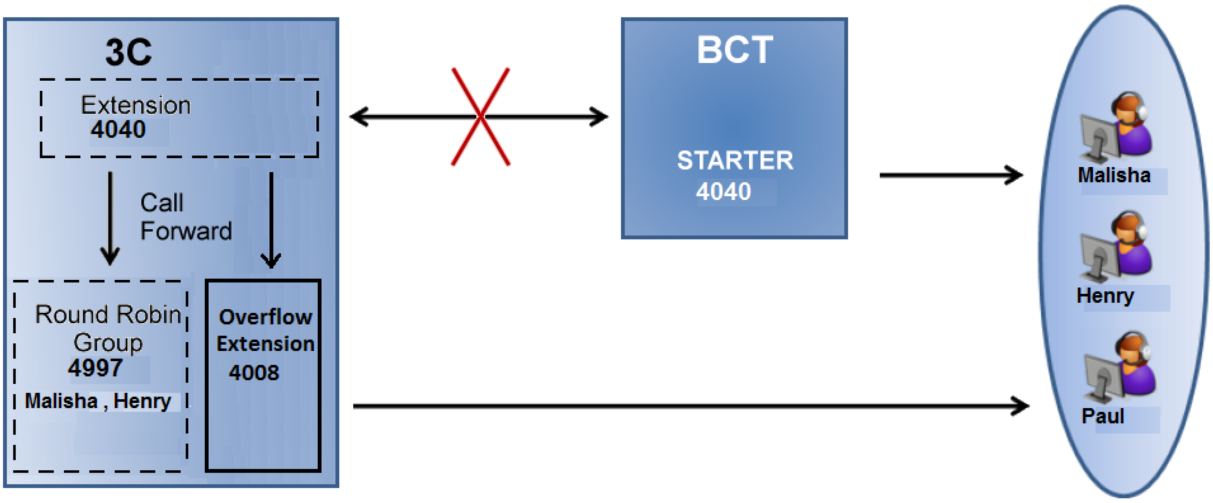
Such a failover can be achieved by configuring overlay round robin groups in UNIVERGE 3C containing operators or agent stations which would normally be controlled by BCT. By configuring BCT starter lines with a call forwarding condition after X rings to those round robin groups a backup is created. When BCT becomes unavailable the starter lines will become deregistered from UNIVERGE 3C. This will force UNIVERGE 3C to follow the call forwarding condition immediately, so calls will be distributed over the agent and operator stations in the round robin groups. If all stations in the round robin group are busy then a second forwarding condition after X+n rings can be programmed to a overflow extension that can handle the calls. This offers limited functionality, but no calls are lost.

24.2.1. Example operation



Under normal condition, BCT and UNIVERGE 3C use a CTI link via web services to communicate. In this example, extension 4040 is a Starter for the Sales in BCT which is directed to a group of Agents. Extension 4040 has Call Forwarding set to extension 4997, which is a Round Robin Group made up of the stations of Agents. A second Call Forwarding is set to extension 4008 to handle calls when all Agent stations in the Round Robin Group are busy.

When a call is made to extension 4040, BCT takes control of the call and routes the call to the Agents.

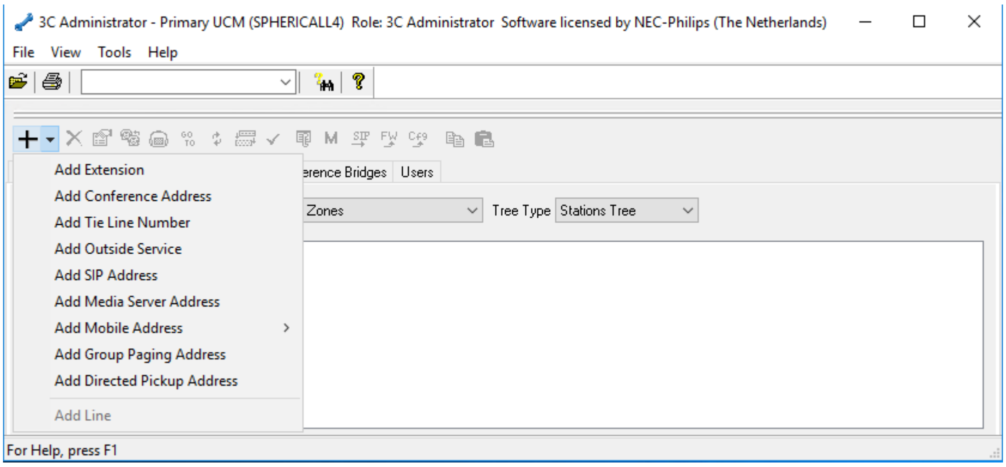


If the CTI link is broken or the BCT isn't working, a call to extension 4040 will immediately forward to Round Robin extension 4997 and be delivered to the station of Agents. When all the stations in the Round Robin group are busy then calls will be forward to extension 4008.

24.2.2. How to assign BCT failover to UNIVERGE 3C

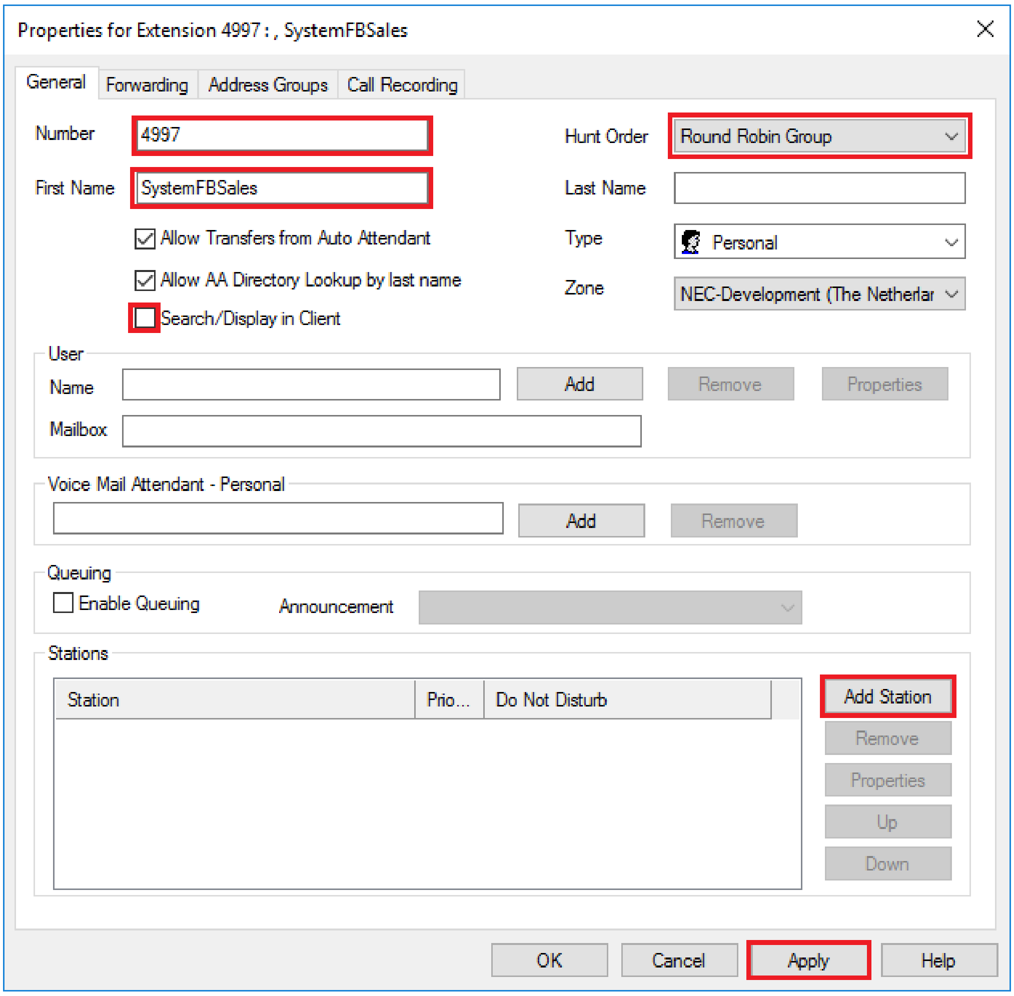
In the UNIVERGE 3C, create a new extension to be used a Round Robin Group whose members will be the BCT Agents. Then set Call Forwarding from the BCT Starter extension to the new Round Robin Group extension.

1. Go to the "Number plan" tab and add a new extension by pressing the down arrow, right from the + icon on the UNIVERGE 3C Administrator toolbar.



2. Now the "Properties for new extension" window appears.

In the Number field, enter "4997".
In the Hunt Order field select "Round Robin Group".
Uncheck the checkbox for "Search/Display in Client".
The First and Last Name fields are optional.



Properties for Extension 4997 : , SystemFBSales

Number: 4997

First Name: SystemFBSales

☑ Allow Transfers from Auto Attendant

☑ Allow AA Directory Lookup by last name

□ Search/Display in Client

Hunt Order: Round Robin Group

Last Name:

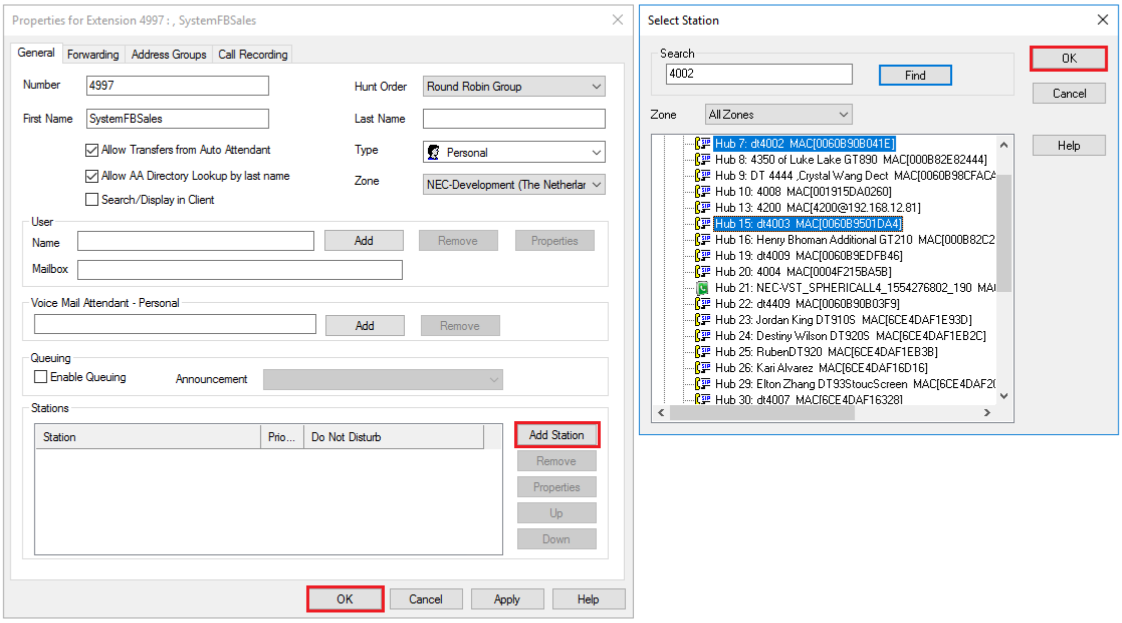
Type: Personal

Zone: NEC-Development (The Netherlar

Queuing: □ Enable Queuing

Station	Prio...	Do Not Disturb

3. Click the **Add station** button. In the **Select Station** window select the Hubs for the Agents from the list (you can use the shift key or control key to make a multiple selection) and click **OK**. The stations are now listed in the "Properties for new extension" window:



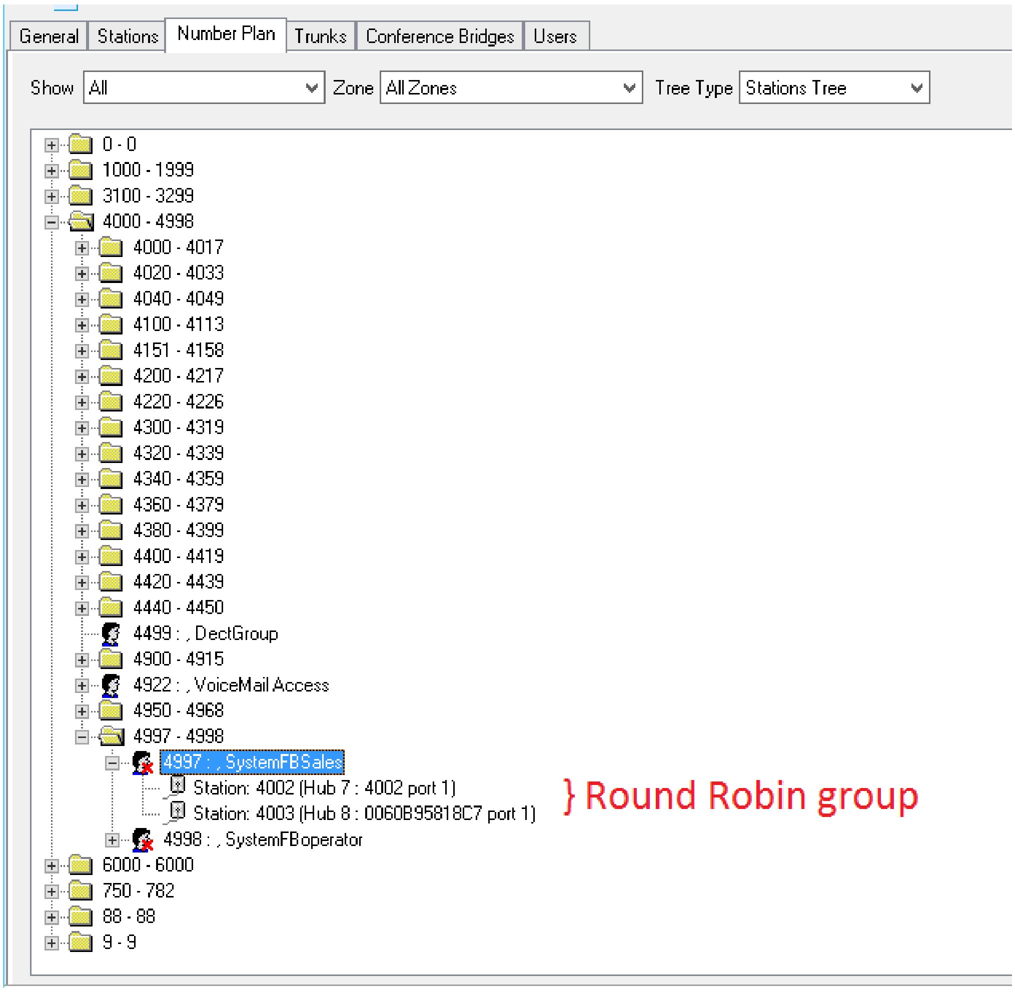
Properties for Extension 4997 : , SystemFBSales

Select Station

Search: 4002

Zone: All Zones

- Hub 7: dt4002 MAC[0060B90B041E]
- Hub 8: 4350 of Luke Lake GT890 MAC[000B82E82444]
- Hub 9: DT 4444 ,Crystal Wang Dect MAC[0060B98CFACA
- Hub 10: 4008 MAC[001915DA0260]
- Hub 13: 4200 MAC[4200@192.168.12.81]
- Hub 15: dt4003 MAC[0060B9501DA4]
- Hub 16: Henry Bhoman Additional GT210 MAC[000B82C2
- Hub 19: dt4009 MAC[0060B9EDFB46]
- Hub 20: 4004 MAC[0004F215BA5B]
- Hub 21: NEC-VST_SPHERICALL4_1554276802_190 MA
- Hub 22: dt4409 MAC[0060B90B03F9]
- Hub 23: Jordan King DT910S MAC[6CE4DAF1E93D]
- Hub 24: Destiny Wilson DT920S MAC[6CE4DAF1EB2C]
- Hub 25: RubenDT920 MAC[6CE4DAF1EB3B]
- Hub 26: Kari Alvarez MAC[6CE4DAF16D16]
- Hub 29: Elton Zhang DT93StoucScreen MAC[6CE4DAF2
- Hub 30: dt4007 MAC[6CE4DAF16328]



Show All

Zone All Zones

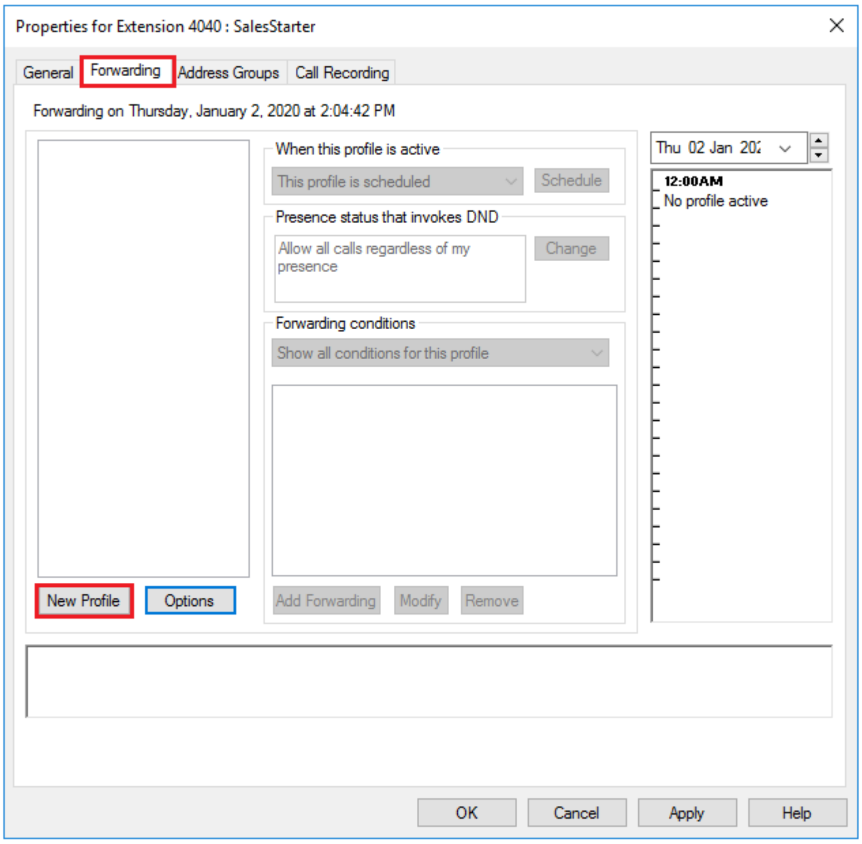
Tree Type Stations Tree

```
0 - 0
1000 - 1999
3100 - 3299
4000 - 4998
    4000 - 4017
    4020 - 4033
    4040 - 4049
    4100 - 4113
    4151 - 4158
    4200 - 4217
    4220 - 4226
    4300 - 4319
    4320 - 4339
    4340 - 4359
    4360 - 4379
    4380 - 4399
    4400 - 4419
    4420 - 4439
    4440 - 4450
    4499 : , DectGroup
    4900 - 4915
    4922 : , VoiceMail Access
    4950 - 4968
    4997 - 4998
        4997 : , SystemFBSales
            Station: 4002 (Hub 7 : 4002 port 1)
            Station: 4003 (Hub 8 : 0060B95818C7 port 1)
        4998 : , SystemFBoperator
6000 - 6000
750 - 782
88 - 88
9 - 9
```

} Round Robin group

4. Set Call Forwarding from the extension used as the BCT Sales Starter (4040 in this example) to the Round Robin group. Select the Number Plan tab and double-click the extension used as the BCT Sales Starter (4040 in this example to show the extension properties.

5. Go to the Forwarding tab and click the New Profile button.



Properties for Extension 4040 : SalesStarter

Forwarding on Thursday, January 2, 2020 at 2:04:42 PM

When this profile is active: This profile is scheduled

Presence status that invokes DND: Allow all calls regardless of my presence

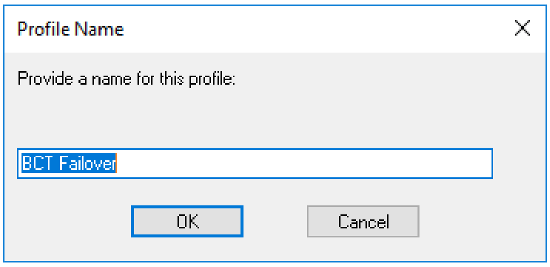
Forwarding conditions: Show all conditions for this profile

Thu 02 Jan 202

12:00AM
No profile active

6. Type a name for the new forwarding profile then click **OK**.

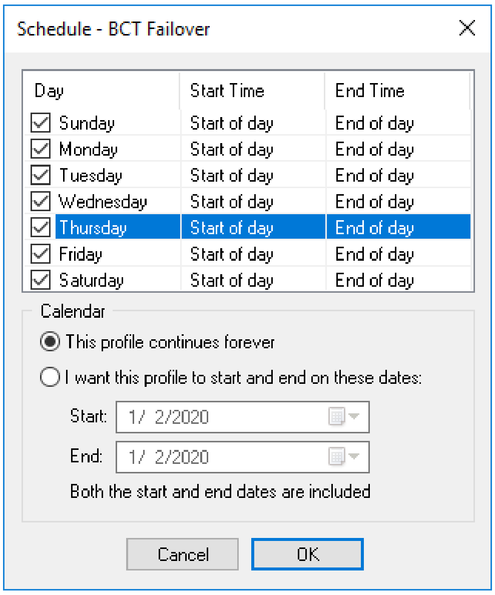
7. In the Schedule window, verify that all days of the week are selected as well as “This profile continues forever”, then click **OK**.



Profile Name

Provide a name for this profile:

BCT Failover



Schedule - BCT Failover

Day	Start Time	End Time
☑ Sunday	Start of day	End of day
☑ Monday	Start of day	End of day
☑ Tuesday	Start of day	End of day
☑ Wednesday	Start of day	End of day
☑ Thursday	Start of day	End of day
☑ Friday	Start of day	End of day
☑ Saturday	Start of day	End of day

Calendar

● This profile continues forever

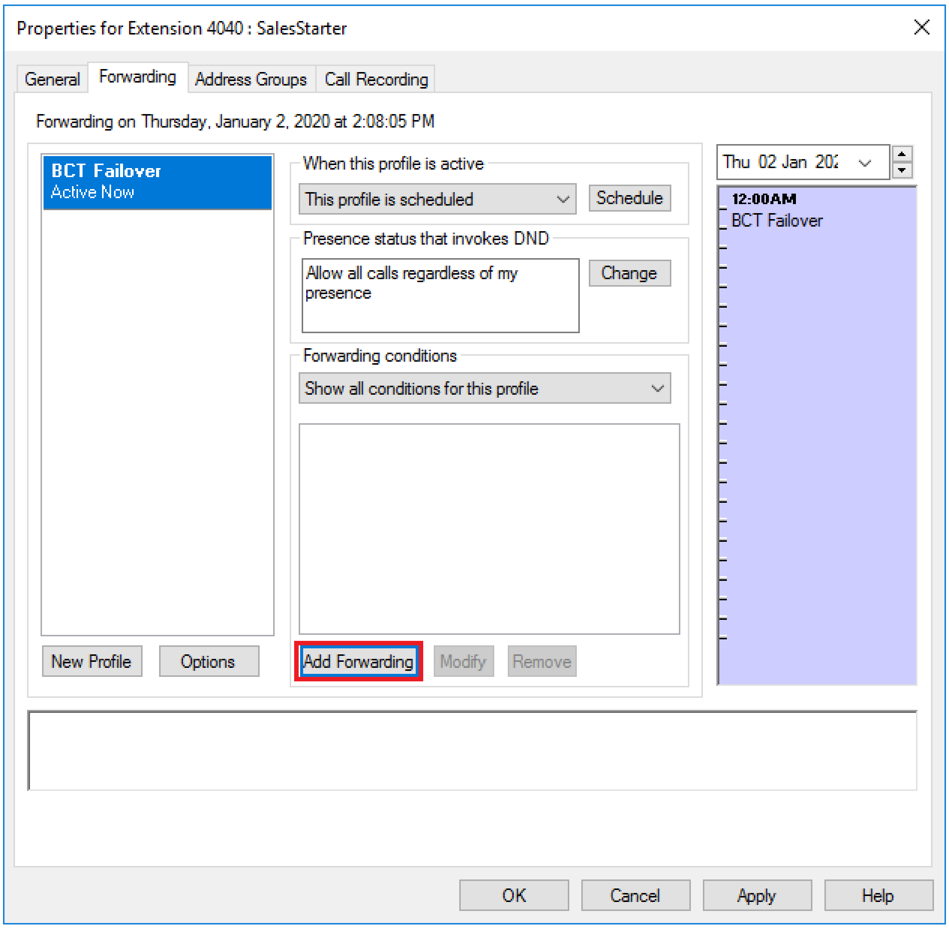
○ I want this profile to start and end on these dates:

Start: 1/ 2/2020

End: 1/ 2/2020

Both the start and end dates are included

8. Click the new forwarding profile to highlight it, then click the Add Forwarding button.



Properties for Extension 4040 : SalesStarter

Forwarding on Thursday, January 2, 2020 at 2:08:05 PM

BCT Failover
Active Now

When this profile is active: This profile is scheduled

Presence status that invokes DND: Allow all calls regardless of my presence

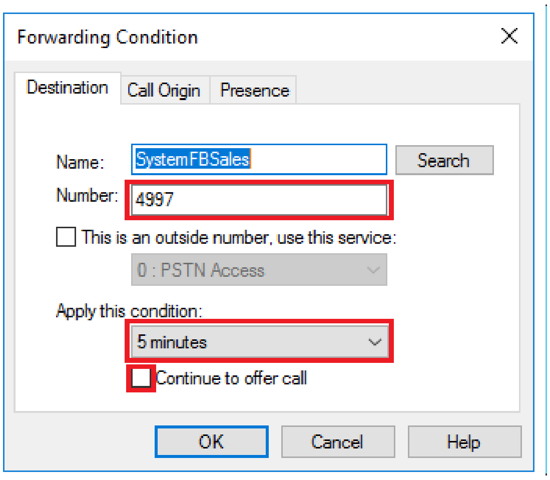
Forwarding conditions: Show all conditions for this profile

Thu 02 Jan 202
12:00AM
BCT Failover

9. Select the Destination tab in the Forwarding Condition window.

- Number:	Enter the number that this Extension will forward to. (4997 in this example)
- Apply this condition:	Use the drop-down menu to select “5 minutes”
- Continue to offer call:	Do Not Check This Option!

Note: the Name is updated after Apply the changes.



Forwarding Condition

Name: SystemFBSales

Number: 4997

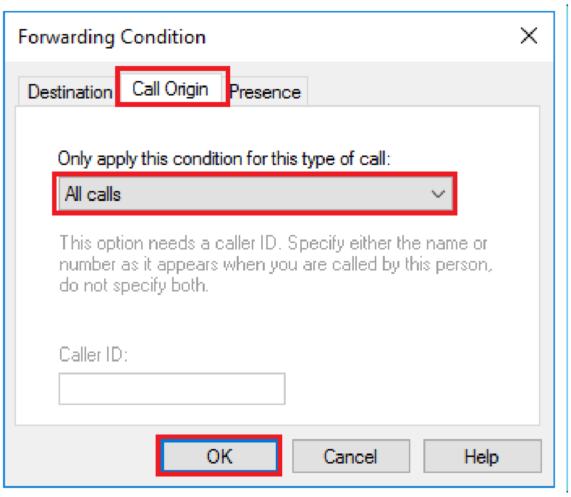
☐ This is an outside number, use this service: 0 : PSTN Access

Apply this condition: 5 minutes

☐ Continue to offer call

Note: *Even though the Call Forwarding timer is set at 5 minutes, if the BCT fails the Call Forwarding will take effect immediately.*

10. Select the Call Origin tab and set the condition to “All calls” and then click OK.



Forwarding Condition

Destination | Call Origin | Presence

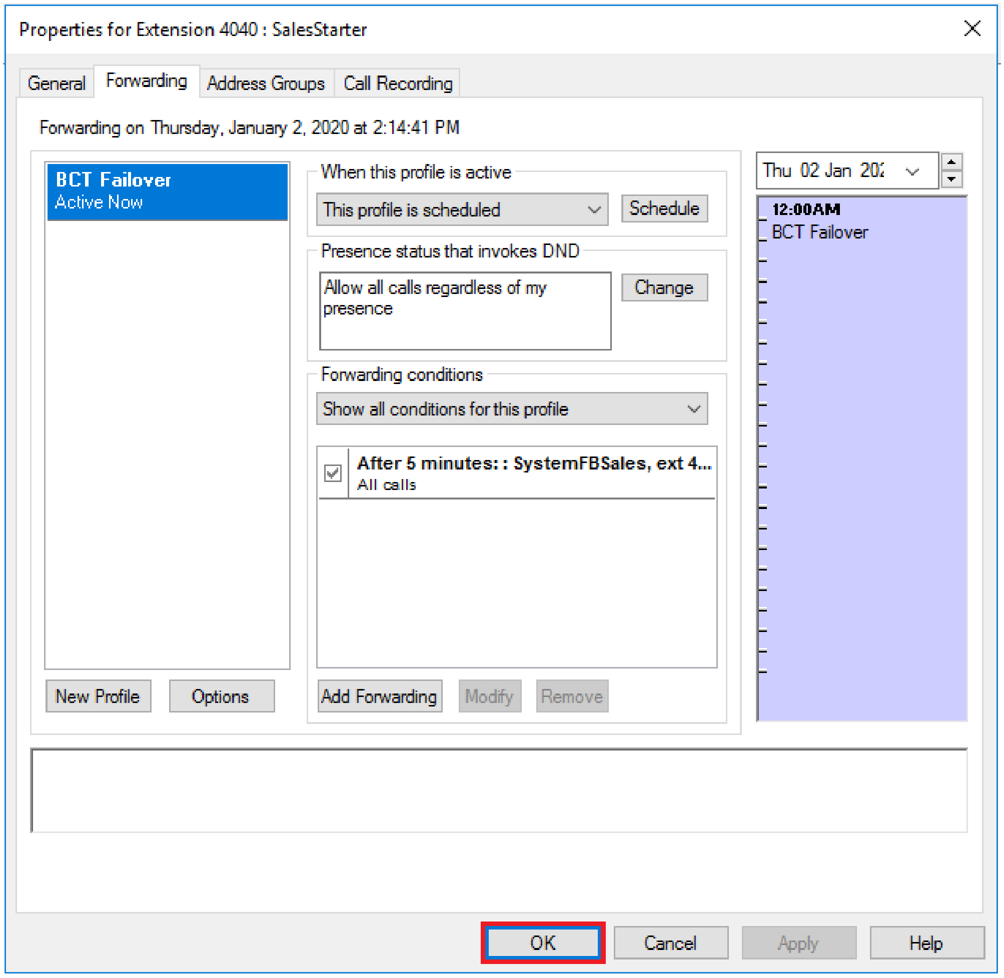
Only apply this condition for this type of call:

All calls

This option needs a caller ID. Specify either the name or number as it appears when you are called by this person, do not specify both.

Caller ID:

11. Select OK to apply the forwarding changes to the extension used as the BCT Sales Starter



Properties for Extension 4040 : SalesStarter

General | Forwarding | Address Groups | Call Recording

Forwarding on Thursday, January 2, 2020 at 2:14:41 PM

BCT Failover
Active Now

When this profile is active: This profile is scheduled

Presence status that invokes DND: Allow all calls regardless of my presence

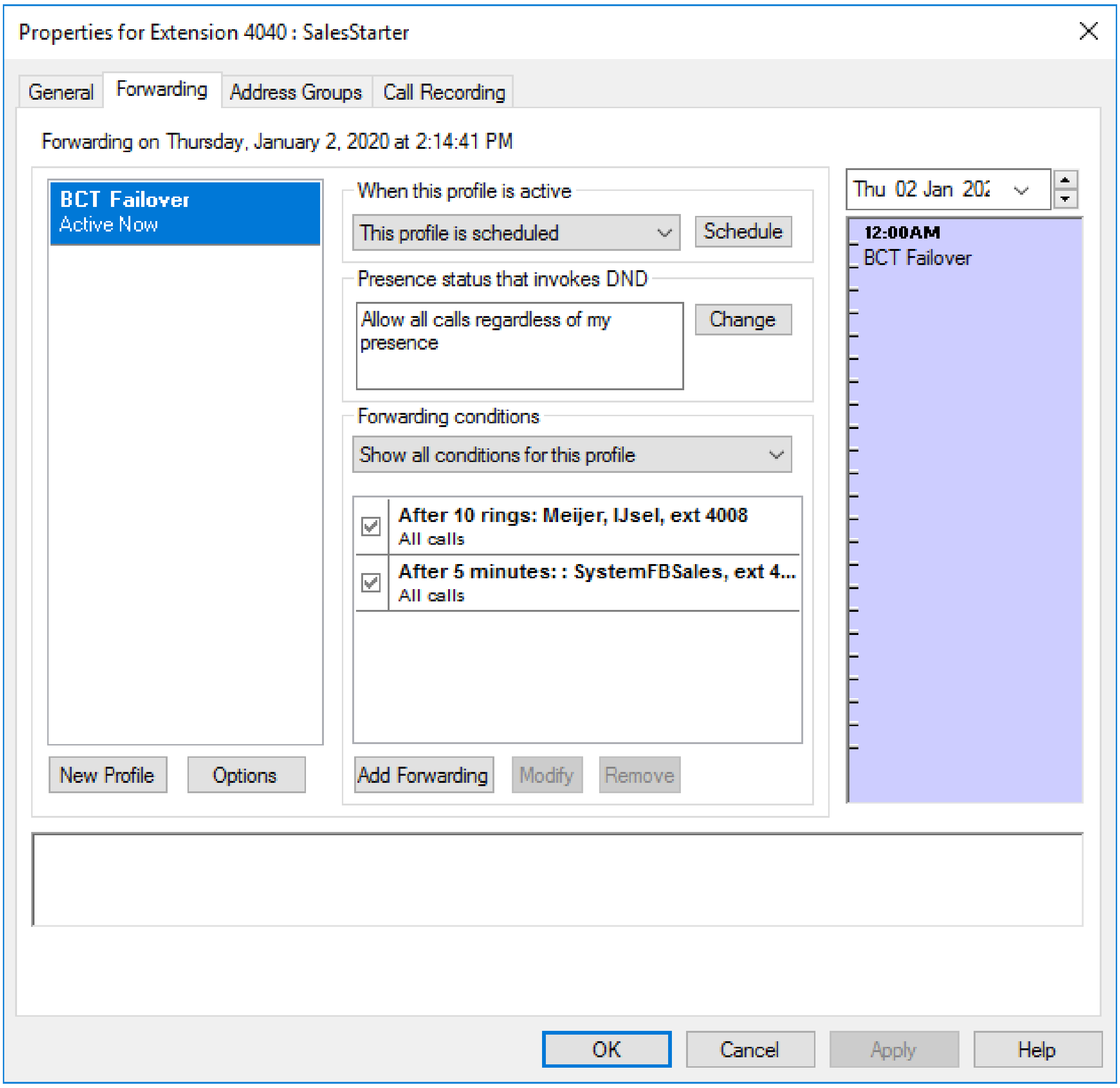
Forwarding conditions: Show all conditions for this profile

☑ After 5 minutes: : SystemFBSales, ext 4...
All calls

Thu 02 Jan 202

12:00AM
BCT Failover

12. To add a second Forwarding condition for the overflow extension press the Add Forwarding button in step 8 and fill in the extension in the Number field and select 10 min in the Apply this condition drop down box. This overflow extension can be configured to handle more calls so calls are queued on this extension.



Properties for Extension 4040 : SalesStarter

Forwarding on Thursday, January 2, 2020 at 2:14:41 PM

BCT Failover
Active Now

When this profile is active: This profile is scheduled

Presence status that invokes DND: Allow all calls regardless of my presence

Forwarding conditions: Show all conditions for this profile

☑ After 10 rings: Meijer, IJsel, ext 4008
All calls

☑ After 5 minutes: : SystemFBSales, ext 4...
All calls

Thu 02 Jan 202

12:00AM
BCT Failover

Note that when calls are queued on this extension and one of the station from the Round Robin group becomes free again then queued calls on the overflow extension are NOT offered to the stations.

13. Repeat this action for other extension used for BCT Starters for Contact centers and operator.

24.3. Appendix N-3 – Configure Presence & Instant Messaging between UNIVERGE 3C and BCT

24.3.1. Configure Presence between UNIVERGE 3C and BCT

Exchange of presence information between UC client/UNIVERGE 3C desktop and BCT client is possible. Per default this is already configured. Otherwise, to configure this, execute the following steps:

On the BCT Server:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\PresenceService.WinService.exe.config”.

2. Locate the key: Sphere

3. Change the value to “on”

4. Press button Save to store the value.

5. Restart the Business ConneCT computer.

24.3.2. Configure Instant Messaging between UNIVERGE 3C and BCT

Instant messaging between UC client/UNIVERGE 3C desktop and BCT client is possible (peer to peer). To configure this, execute the following steps:

On the BCT Server:

1. Open the Configuration Manager and select the configuration file “C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config.

2. Locate the key: SphericallMessaging

3. Change value to “on”

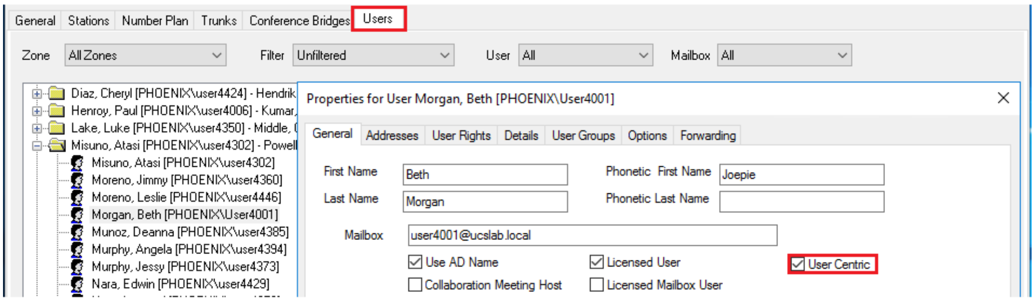
4. Press button Save to store the value.

5. Restart the Business ConneCT computer.

24.3.3. Configure users in UNIVERGE 3C for Presence & IM

Any user that will be utilizing Presence and/or IM must be set as User Centric and also assigned to a User Group. And to allow BCT to see 3C user’s presence states, the CTIuser must have monitor rights on these User Groups.

1. To set a user to User Centric, from the 3C Administrator open the Users Tab, right-click the user to be modified and select View Properties from the pop-up menu. In the Properties menu select the General Tab and check the User Centric check box.



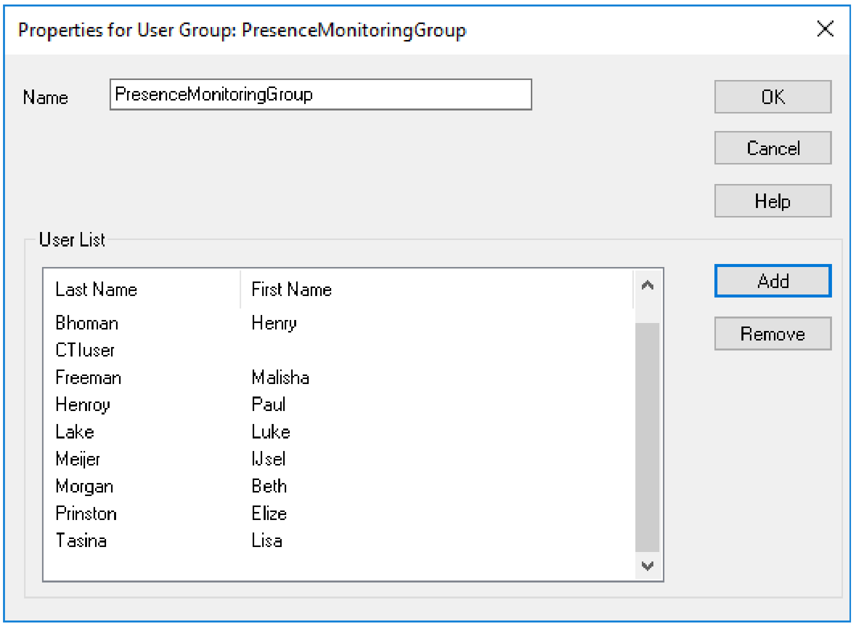
Zone: All Zones
Filter: Unfiltered
User: All
Mailbox: All

Diaz, Cheryl [PHOENIX\user4424] - Hendrik
Henroy, Paul [PHOENIX\user4006] - Kumar,
Lake, Luke [PHOENIX\user4350] - Middle,
Misuno, Atasi [PHOENIX\user4302] - Powell
Misuno, Atasi [PHOENIX\user4302]
Moreno, Jimmy [PHOENIX\user4360]
Moreno, Leslie [PHOENIX\user4446]
Morgan, Beth [PHOENIX\User4001]
Munoz, Deanna [PHOENIX\user4385]
Murphy, Angela [PHOENIX\user4394]
Murphy, Jessy [PHOENIX\user4373]
Nara, Edwin [PHOENIX\user4429]

Properties for User Morgan, Beth [PHOENIX\User4001]

First Name: Beth
Last Name: Morgan
Phonetic First Name: Joepie
Phonetic Last Name:
Mailbox: user4001@ucslab.local
☑ Use AD Name
☑ Licensed User
☑ User Centric
☐ Collaboration Meeting Host
☐ Licensed Mailbox User

2. To add users to a User Group, from the 3C Administrator open the General Tab and expand the User Lists and select User Groups. Either right-click User Groups and select Add to create a new User Group or open the properties of an existing User Group to add new users to it.



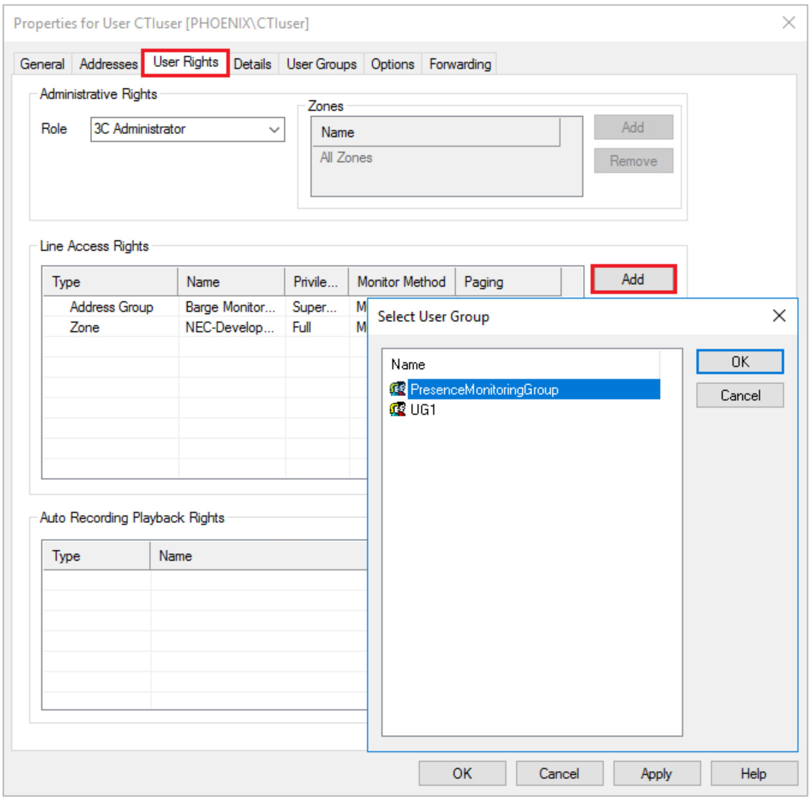
Name: PresenceMonitoringGroup

User List

Last Name	First Name
Bhoman	Henry
CTIuser	
Freeman	Malisha
Henroy	Paul
Lake	Luke
Meijer	IJsel
Morgan	Beth
Prinston	Elize
Tasina	Lisa

3. To allow CTIuser to monitor these User Groups, open the Users Tab in the 3C Administrator, right-click on the CTIuser and select View properties from the pop-up menu. In the Properties menu select the User Rights tab, click Add, User Group and select one or more User Groups.

***Note**: CTIuser must be set to User Centric. See chapter 4.6.4.9 Configure CTIuser.*



Administrative Rights

Role: 3C Administrator

Zones

Name
All Zones

Line Access Rights

Type	Name	Privile...	Monitor Method	Paging
Address Group	Barge Monitor...	Super...	M	
Zone	NEC-Develop...	Full	M	

Auto Recording Playback Rights

Type	Name

Name
PresenceMonitoringGroup
UG1

24.3.4. Presence between UC Client and BCT Client

The charts below show what will be displayed on the UC Client and BCT Client for various presence states.

State of UC Client	BCT Client Displays
Online	Online
Away	Away From Computer
Be Right Back	Away From Computer
Busy	Busy
Out to Lunch	Away From Computer
Out of Office	Offline
In A Meeting	Busy
DND	Do Not Disturb
Offhook	Busy-In a Call
Invisible	Offline
Offline	Offline

State of BCT Client	UC Client Displays
Ready	Online
Not Ready	Online
Offhook	On the Phone
No Activity	Away
Offline	Offline

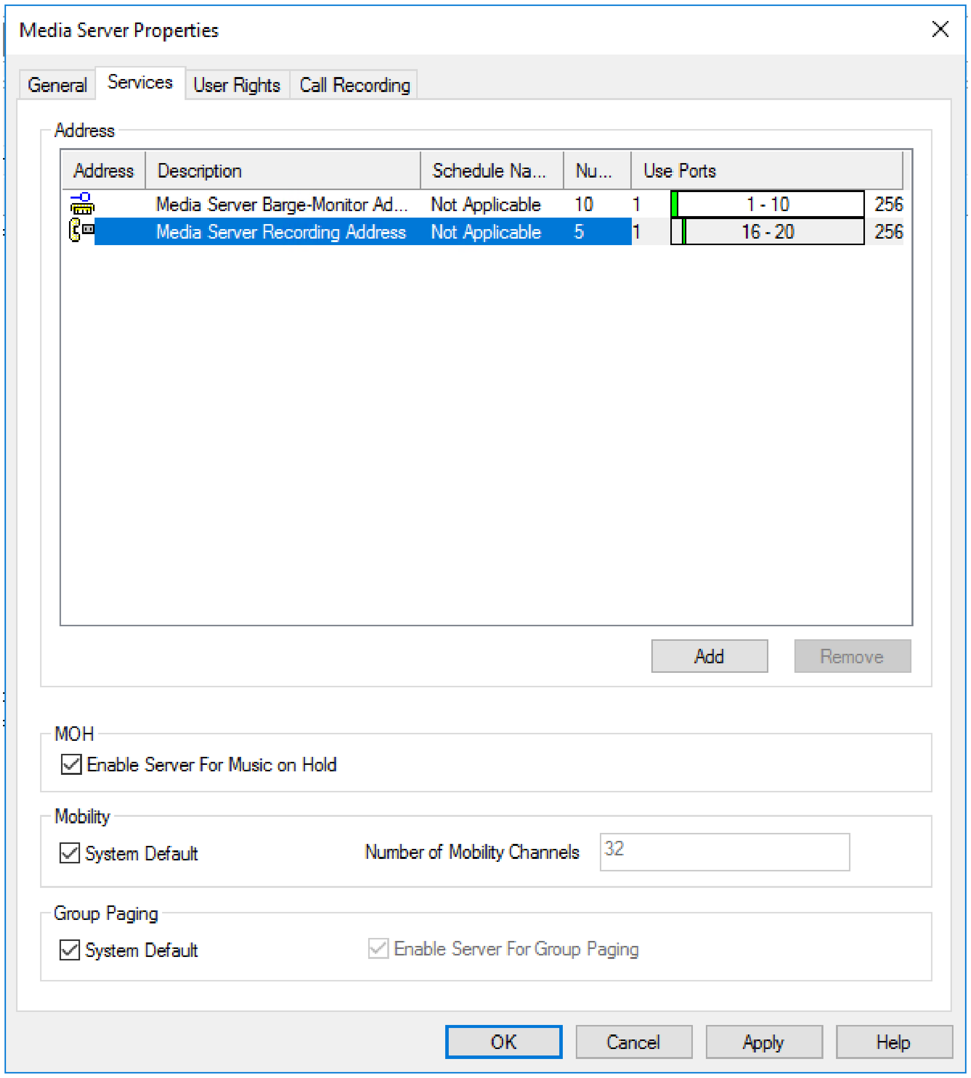
24.4. Appendix N-4 – Operator Break-In

One special case of call control is the operator break-in facility. For this to work, the operator users needs to be configured for the UNIVERGE 3C Barge-Monitor.

One important aspect of the configuration in UNIVERGE 3C is that extensions that can be barged into as well as extensions that will initiate the barge-in have to be members of the same address group. Users allowed to initiate a barge-in session need to have supervision rights to this address group.

Crucial is that also the CTIuser needs to be given these supervision rights to any address group configured for barge-monitor, otherwise the CTIuser is not allowed to start a barge-in session (operator break-in) on behalf of a BCT operator client.

24.4.1. Set the Media Server Barge Monitor Address



Address	Description	Schedule Na...	Nu...	Use Ports		
	Media Server Barge-Monitor Ad...	Not Applicable	10	1	1 - 10	256
	Media Server Recording Address	Not Applicable	5	1	16 - 20	256

☑ Enable Server For Music on Hold

☑ System Default

Number of Mobility Channels 32

☑ System Default

☑ Enable Server For Group Paging

1. In the UNIVERGE 3C Administrator, Select the General tab.

2. Select Media Servers from the list.

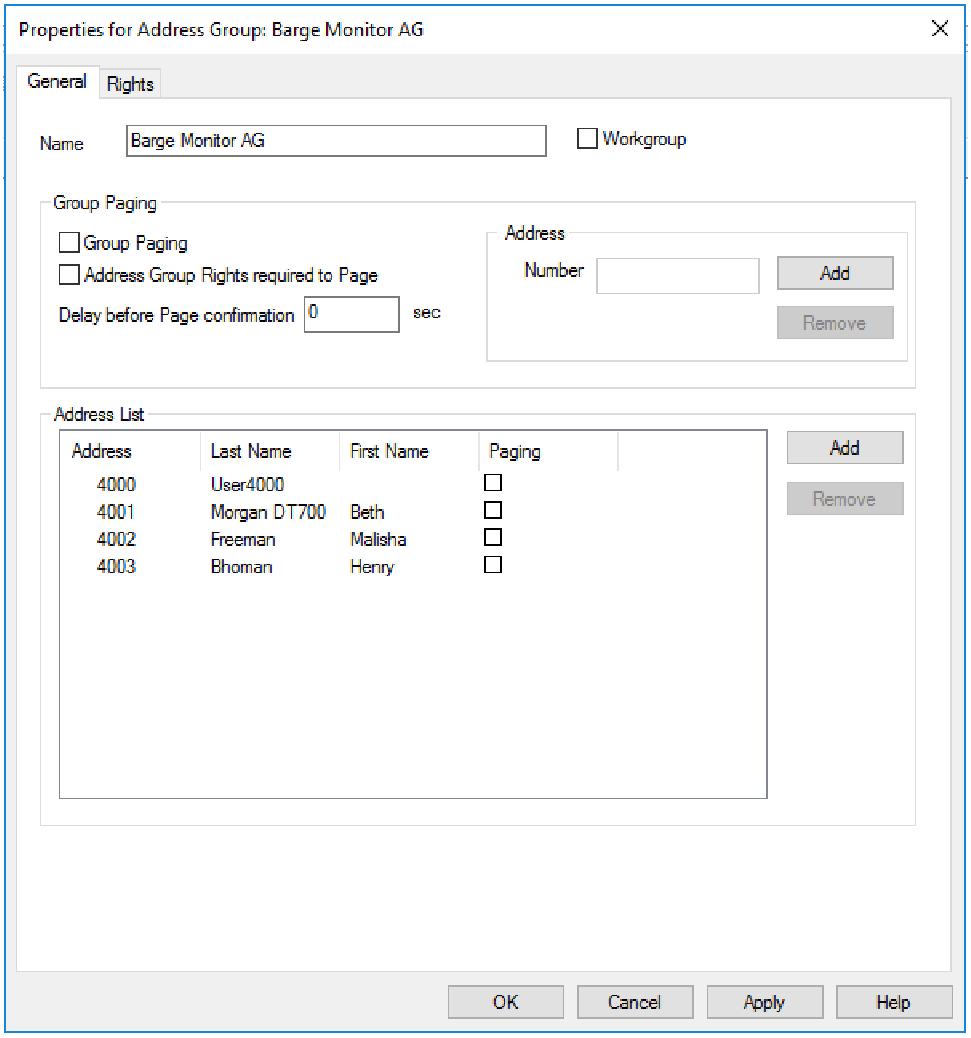
3. Right-click the Media Server that is used for Barge-Monitor and then select View Properties.

4. Select the Services tab.

5. Adjust the number of ports as needed for your system. At least 1 port must be configured with the Barge-Monitor address.

6. Click **OK** to save.

24.4.2. Address Group configuration



Properties for Address Group: Barge Monitor AG

Name: Barge Monitor AG □ Workgroup

Group Paging

□ Group Paging

□ Address Group Rights required to Page

Delay before Page confirmation: 0 sec

Address

Number:

Address List

Address	Last Name	First Name	Paging
4000	User4000		□
4001	Morgan DT700	Beth	□
4002	Freeman	Malisha	□
4003	Bhoman	Henry	□

1. In the UNIVERGE 3C Administrator, Select the General tab.

2. Right-Click Address Groups and select Add.

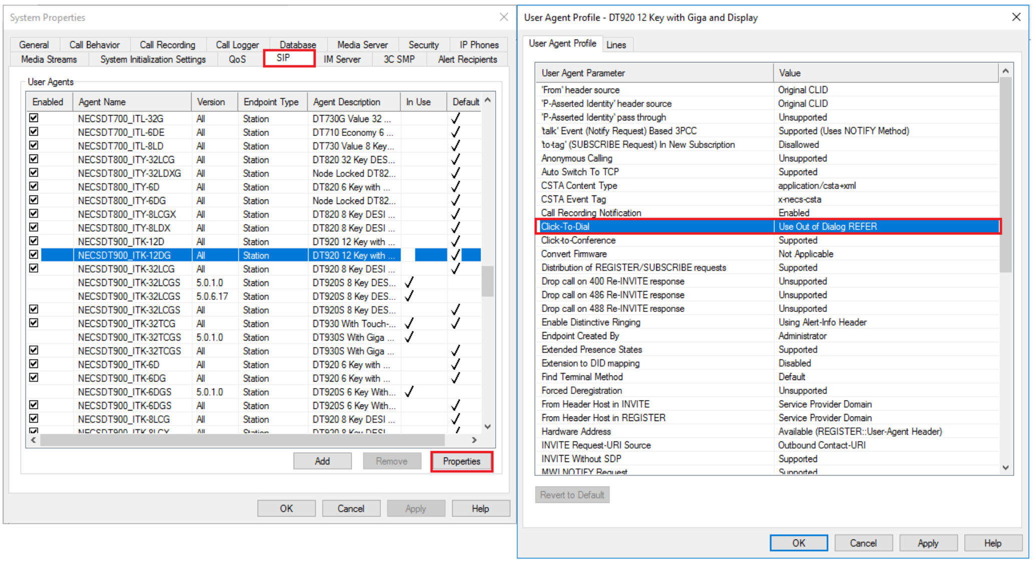
3. In the General tab enter an appropriate, unique name for the Address Group in the Name field.

4. Under Address List, click Add and choose all extensions to which Break-In will be allowed, including the Operator.

5. In the Rights tab press Add to add the operator users; double click on one of the operator users to reveal the User Rights of the user. Now double click the Privilege column of the Address group and select Supervise from the drop down list. Press Ok to close the User properties.

6. Click **OK** to save.

24.4.3. Set “Out of Dialog REFER”



Enabled	Agent Name	Version	Endpoint Type	Agent Description	In Use	Default
☑	NECSDT700_ITL-32G	All	Station	DT730G Value 32 ...		✓
☑	NECSDT700_ITL-6DE	All	Station	DT710 Economy 6 ...		✓
☑	NECSDT700_ITL-8LD	All	Station	DT730 Value 8 Key...		✓
☑	NECSDT800_ITY-32LCG	All	Station	DT820 32 Key DES...		✓
☑	NECSDT800_ITY-32LDXG	All	Station	Node Locked DT82...		✓
☑	NECSDT800_ITY-6D	All	Station	DT820 6 Key with ...		✓
☑	NECSDT800_ITY-6DG	All	Station	Node Locked DT82...		✓
☑	NECSDT800_ITY-8LCGX	All	Station	DT820 8 Key DESI ...		✓
☑	NECSDT800_ITY-8LDX	All	Station	DT820 8 Key DESI ...		✓
☑	NECSDT900_ITK-12D	All	Station	DT920 12 Key with ...		✓
☑	NECSDT900_ITK-12DG	All	Station	DT920 12 Key with ...		✓
☑	NECSDT900_ITK-32LCG	All	Station	DT920 8 Key DESI ...		✓
	NECSDT900_ITK-32LCGS	5.0.1.0	Station	DT920S 8 Key DES...	✓	
	NECSDT900_ITK-32LCGS	5.0.6.17	Station	DT920S 8 Key DES...	✓	
☑	NECSDT900_ITK-32LCGS	All	Station	DT920S 8 Key DES...		✓
☑	NECSDT900_ITK-32TCG	All	Station	DT930 With Touch-...	✓	✓
	NECSDT900_ITK-32TCGS	5.0.1.0	Station	DT930S With Giga ...	✓	
☑	NECSDT900_ITK-32TCGS	All	Station	DT930S With Giga ...		✓
☑	NECSDT900_ITK-6D	All	Station	DT920 6 Key with ...		✓
☑	NECSDT900_ITK-6DG	All	Station	DT920 6 Key with ...		✓
	NECSDT900_ITK-6DGS	5.0.1.0	Station	DT920S 6 Key With...	✓	
☑	NECSDT900_ITK-6DGS	All	Station	DT920S 6 Key With...		✓
☑	NECSDT900_ITK-8LCG	All	Station	DT920 8 Key DESI ...		✓
☑	NECSDT900_ITK-8LCX	All	Station	DT920 8 Key DESI		✓

User Agent Parameter	Value
'From' header source	Original CLID
'P-Asserted Identity' header source	Original CLID
'P-Asserted Identity' pass through	Unsupported
'talk' Event (Notify Request) Based 3PCC	Supported (Uses NOTIFY Method)
'to-tag' (SUBSCRIBE Request) In New Subscription	Disallowed
Anonymous Calling	Unsupported
Auto Switch To TCP	Supported
CSTA Content Type	application/csta+xml
CSTA Event Tag	x-necs-csta
Call Recording Notification	Enabled
Click-To-Dial	Use Out of Dialog REFER
Click-to-Conference	Supported
Convert Firmware	Not Applicable
Distribution of REGISTER/SUBSCRIBE requests	Supported
Drop call on 400 Re-INVITE response	Unsupported
Drop call on 486 Re-INVITE response	Unsupported
Drop call on 488 Re-INVITE response	Unsupported
Enable Distinctive Ringing	Using Alert-Info Header
Endpoint Created By	Administrator
Extended Presence States	Supported
Extension to DID mapping	Disabled
Find Terminal Method	Default
Forced Deregistration	Unsupported
From Header Host in INVITE	Service Provider Domain
From Header Host in REGISTER	Service Provider Domain
Hardware Address	Available (REGISTER::User-Agent Header)
INVITE Request-URI Source	Outbound Contact-URI
INVITE Without SDP	Supported
MWI NOTIFY Request	Supported

1. In the UNIVERGE 3C Administrator, Select the General tab.

2. Right-Click on the System name and choose View Properties.

3. Select the SIP tab.

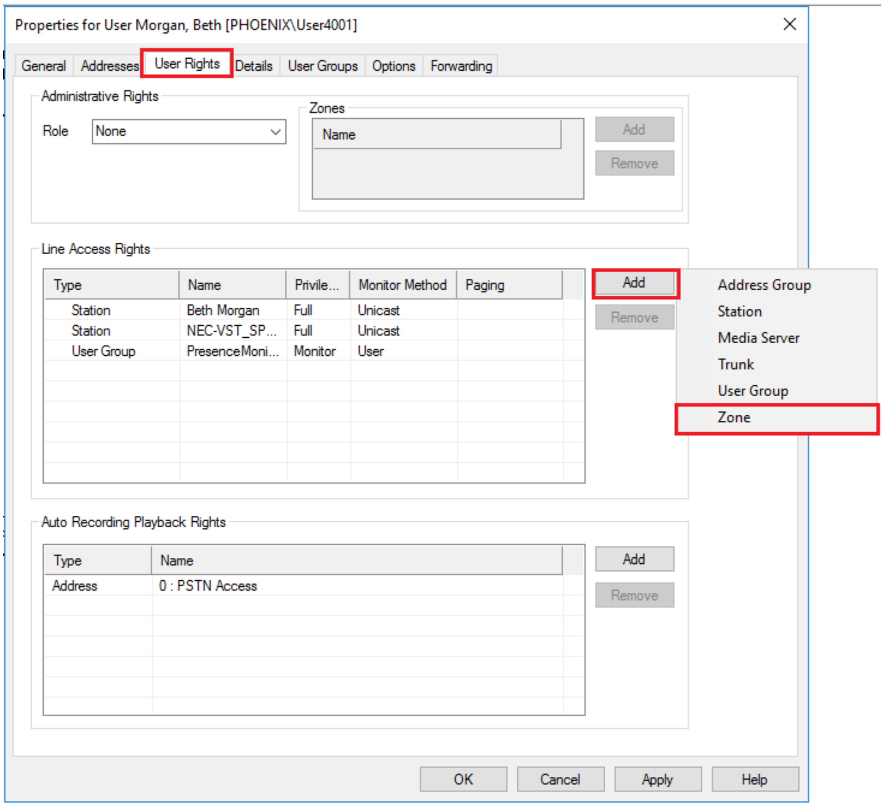
4. Click to highlight the appropriate Agent Name (phone type) used by the Operator.

5. Click the Properties button.

6. For Click-To-Dial, choose Use Out of Dialog REFER from the pull-down menu.

7. Click **OK** to save.

24.4.4. Add Supervisor (Operator) user rights



Role: None

Zones

Name

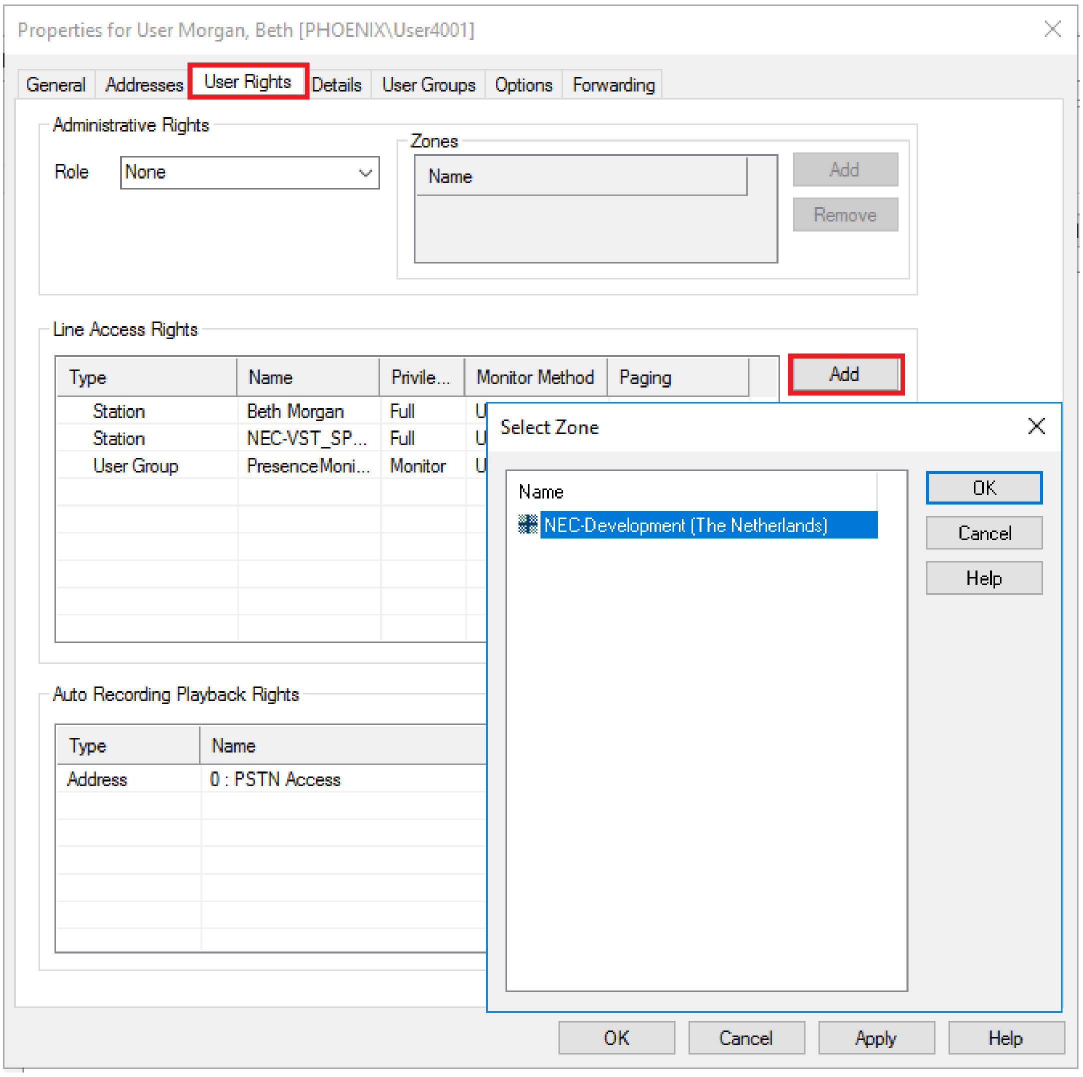
Line Access Rights

Type	Name	Privile...	Monitor Method	Paging
Station	Beth Morgan	Full	Unicast	
Station	NEC-VST_SP...	Full	Unicast	
User Group	PresenceMoni...	Monitor	User	

Auto Recording Playback Rights

Type	Name
Address	0 : PSTN Access

1. In the UNIVERGE 3C Administrator, Select the User tab.
2. Double-Click the user which will be the BCT Operator.
3. Select the User Rights tab.
4. Verify that the user have Full Privileges for themselves in Line Access Rights.
5. Click **Add** and select Zone.



Role: None

Name

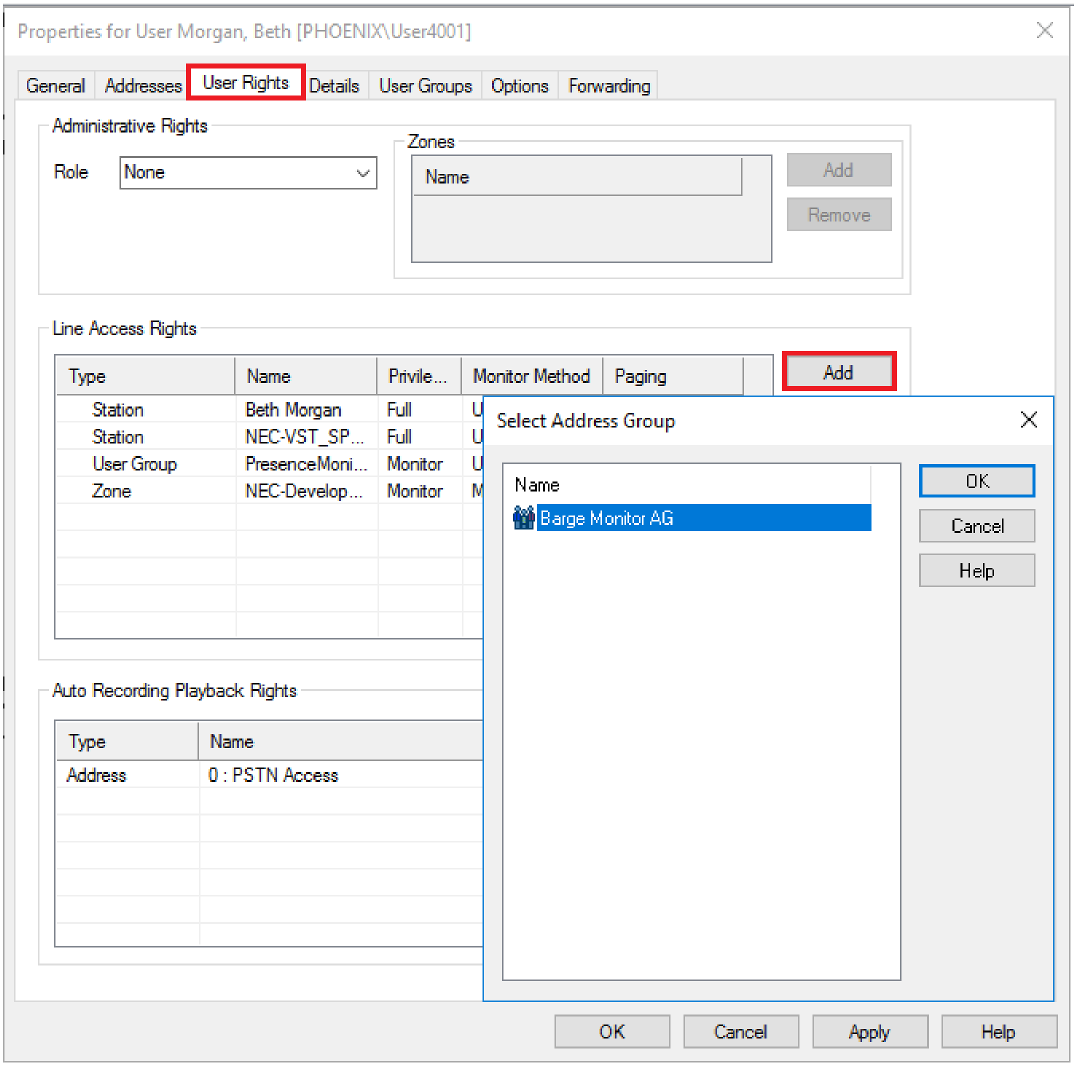
Type	Name	Privile...	Monitor Method	Paging
Station	Beth Morgan	Full	U	
Station	NEC-VST_SP...	Full	U	
User Group	PresenceMoni...	Monitor	U	

Type	Name
Address	0 : PSTN Access

Name
NEC-Development (The Netherlands)

6. Select the Zone which Break-In should work and click OK.

7. Verify that the Privilege level is set to Monitor.



Properties for User Morgan, Beth [PHOENIX\User4001]

Role: None

Name

Type	Name	Privile...	Monitor Method	Paging
Station	Beth Morgan	Full	U	
Station	NEC-VST_SP...	Full	U	
User Group	PresenceMoni...	Monitor	U	
Zone	NEC-Develop...	Monitor	M	

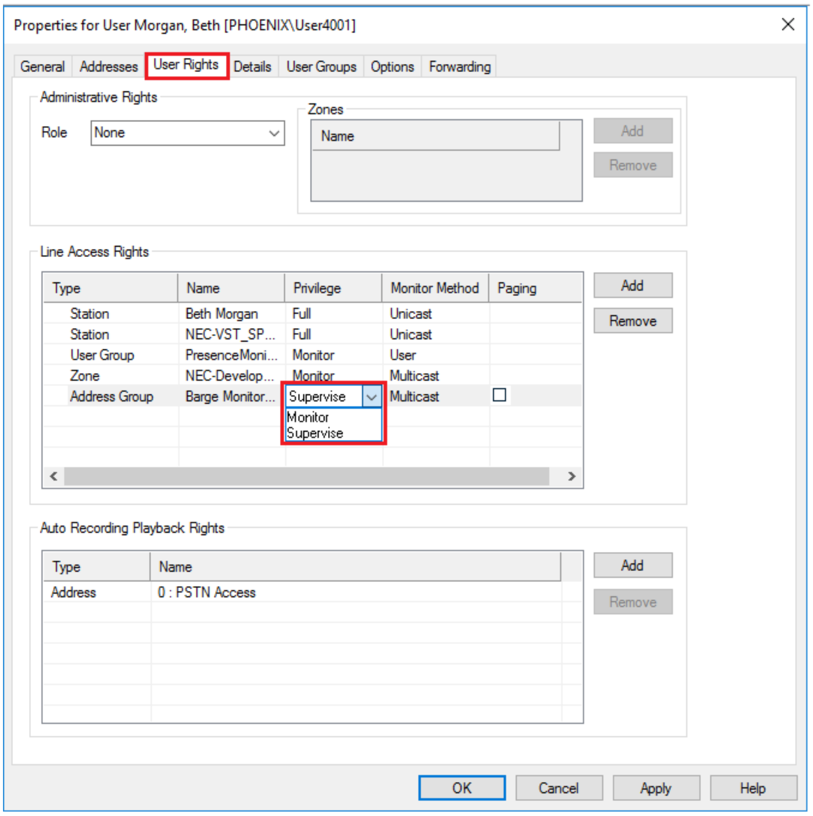
Type	Name
Address	0 : PSTN Access

Select Address Group

Name
Barge Monitor AG

8. Click Add and select Address Group.

9. Select the Address Group created for Break-In and click **OK**.



Properties for User Morgan, Beth [PHOENIX\User4001]

General | Addresses | User Rights | Details | User Groups | Options | Forwarding

Administrative Rights

Role: None

Zones

Name

Line Access Rights

Type	Name	Privilege	Monitor Method	Paging
Station	Beth Morgan	Full	Unicast	
Station	NEC-VST_SP...	Full	Unicast	
User Group	PresenceMoni...	Monitor	User	
Zone	NEC-Develop...	Monitor	Multicast	
Address Group	Barge Monitor...	Supervise Monitor Supervise	Multicast	□

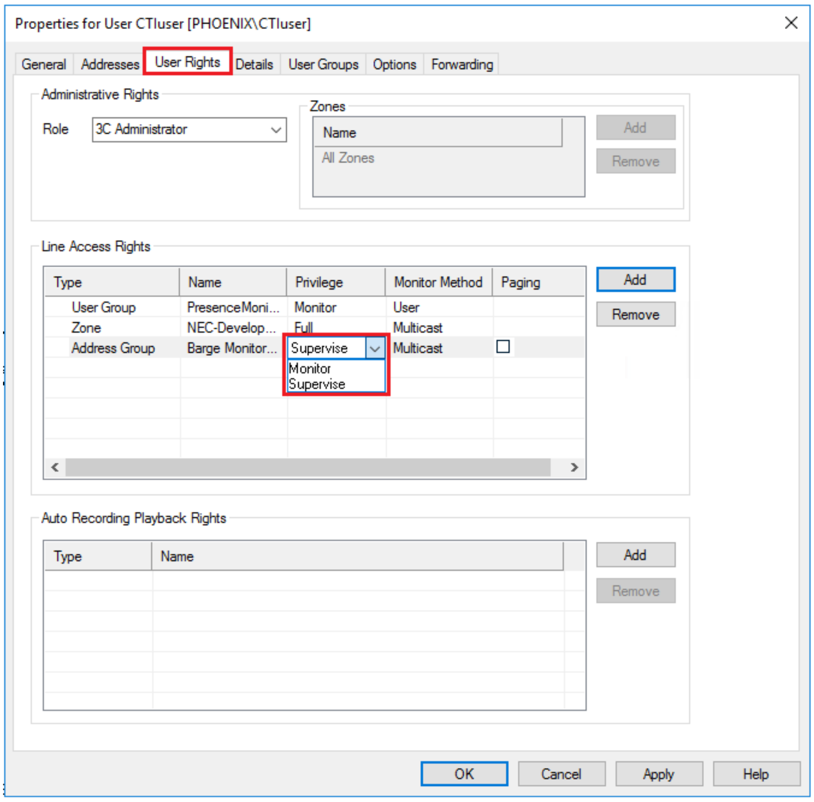
Auto Recording Playback Rights

Type	Name
Address	0 : PSTN Access

10. Use the pull-down menu to change the Privilege level to Supervise.

11. Click **OK** to save.

12. Repeat steps 8-11 for CTIuser.



Properties for User CTIuser [PHOENIX\CTIuser]

General | Addresses | User Rights | Details | User Groups | Options | Forwarding

Administrative Rights

Role: 3C Administrator

Zones

Name
All Zones

Line Access Rights

Type	Name	Privilege	Monitor Method	Paging
User Group	PresenceMoni...	Monitor	User	
Zone	NEC-Develop...	Full	Multicast	
Address Group	Barge Monitor...	Supervise Monitor Supervise	Multicast	□

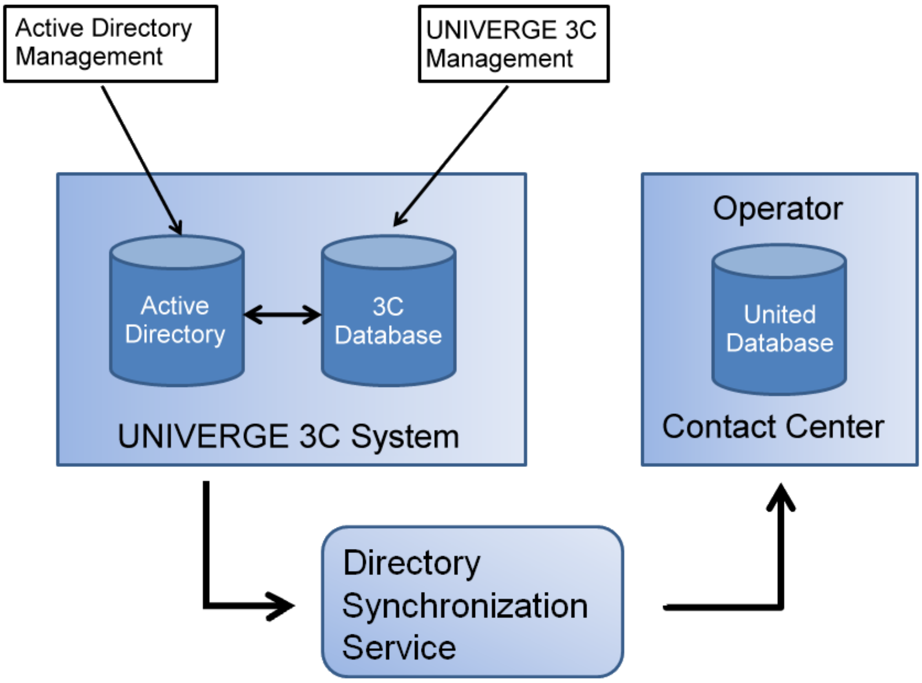
Auto Recording Playback Rights

Type	Name

24.5. Appendix N-5 – Active Directory synchronization

The UNIVERGE 3C system is tightly integrated into an Active Directory Domain Infrastructure. Extensions which will be used by BCT are assigned by the UNIVERGE 3C to Domain Users. Information about BCT Operator and Contact Center users exists in both the UNIVERGE 3C database and in Active Directory. When a BCT synchronization is performed, it will copy information from both UNIVERGE 3C and Active Directory into the BCT United Database. Synchronization is done during installation of the BCT server. Once BCT is installed, you can manually synchronize via the Connectivity tab in the BCT System Settings window.

The (UNIVERGE 3C system) administrator can add users to the Active Directory with the management tool “Active Directory Users and Computers”. After that the user has to be assigned to an extension with the “UNIVERGE 3C Administrator”. The last step is synchronizing this data towards BCT with the “Directory Synchronization Service”.



24.5.1. Active Directory mapping

The information that BCT collects from Active Directory is used to populate fields in the Company Directory. Not every field in the Company Directory is populated with data from Active Directory. The chart below shows which fields are populated from Active Directory.

Note: *Changes to these fields can only be made in Active Directory.*

BCT Company Directory Field	Active Directory	
	Field Name	**Attribute Name**
Building	Office	physicalDeliveryOfficeName
Company	Company	company
Department	Department	department
Division [optional]	--	division
Email	Email	mail
Fax	Fax	facsimileTelephoneNumber
Home City	City	l (*lower case L*)
Home Address 1	Street	streetAddress
Home Phone	Home	homePhone
Home State	State	st
Home Zip Code	Zip/Postal Code	postalCode
Jobtitle	Job Title	title
Middle Name	--	middleName
Mobile Phone	Mobile	mobile
NT Login	Domain Name	sAMAccountName
Pager	Pager	pager
Title [optional]	--	personalTitle

Note that the Company-, optionally Division- and Department-fields, collected from Active Directory, represent the hierarchy information, which is used to populate the Group Lists used in BCT.

24.5.2. LDAP Filtering

By default BCT will collect all Active Directory users and will then populate the data for the users that were synchronized from UNIVERGE 3C. When there are a lot of users in Active Directory then the whole synchronization process might take a lot of time. You can reduce this by defining an LDAP filter on the query.

The Directory Synchronization Service supports 2 levels of filtering: container and object. For example you can specify from which organizational units to read from and also the match criteria for users. The LDAP filter syntax is based on RFC-4515, for more information see LDAP Query Basics [http://technet.microsoft.com/aa996205]

Some examples:

Type	LDAP filter	Description
Container	(&(objectClass=organizationalUnit)(ou=Affairs))	Only organizational unit "Affairs"
Container	(&(objectClass=organizationalUnit)(!(ou=External))(!(ou=Customers)))	All organizational units except "External" and "Customers"
Object	(&(objectCategory=person)(objectClass=user)(|(cn=fred*)(cn=*kit*)))	All users with a common name starting with "fred" or containing "kit"
Object	(&(objectCategory=person)(objectClass=user)(userPrincipalName=*))	Only users with a User Principal Name

To define a custom LDAP filter:

1. Browse to "C:\Program Files (x86)\Common Files\NEC\Services" and use a text editor (e.g. Notepad) to open the file "DirSyncService.config"

2. Search for the section "LDAPOptions" and enter the LDAP filter in the appropriate Filter attribute: Container for organizational units and Object for users.

   Note**: Make sure to escape XML markup characters, for example **&** should be written as **&amp;

3. Save and close the file

4. Restart the service "NEC Directory Synchronization Service"

5. Synchronize the 3C PBX

24.5.3. Extend LDAP search

A typical BCT environment is an Active Directory domain with a single Domain Controller. Only users from that Domain Controller are configured in UNIVERGE 3C. Any Active Directory user outside this Domain Controller will not be detected by the BCT synchronization process.

When you have child domains (tree) in your Active Directory domain and users from the child domain(s) are configured in UNIVERGE 3C then you need to extend the LDAP search focus. This allows the BCT directory synchronization process to receive user information from the child domains as well.

To extend the search focus:

1. Browse to "`C:\Program Files (x86)\Common Files\NEC\Services`" and use a text editor (e.g. Notepad) to open the file "DirSyncService.config"

2. Search for the section "LDAPOptions" and find the attribute `SearchOption` under Object. Change the value to `PhantomRoot`

3. Save and close the file

4. Restart the service "NEC Directory Synchronization Service"

5. Synchronize the 3C PBX

Side notes about the PhantomRoot option:

- The time for the synchronization process might increase considerably as more users need to be read.
- Once enabled, the users will be fetched from the Global Catalog. Therefore the available user attributes is limited to what is defined in the Partial Attribute Set (PAS). Some less common attributes like company and department are not available for users that reside in a different domain controller.

The attributes that are not synchronized by default:

- middleName, personalTitle;

- company, department, departmentNumber;

- facsimileTelephoneNumber, mobile, pager;

- physicalDeliveryOfficeName, streetAddress, postalCode;
- wWWHomePage;

You can however choose to include this in the PAS with the MMC add-in "Active Directory Schema". In Attributes select the ones that you want to be replicated and check the "Replicate" checkbox in properties. It might take a couple of minutes for the Domain Controllers to replicate the new attributes.

24.6. Appendix N-6 – Test the BCT / UNIVERGE 3C configuration

24.6.1. Test CTIuser

If the BCT Synchronization to UNIVERGE 3C and Active Directory succeeded during the initial configuration of BCT via the Configuration Wizard, then the CTIuser is created and configured properly in Active Directory.

24.6.2. Verify Operator Queues

1. Log in an operator client.

2. From a UNIVERGE 3C terminal make an internal call to the operator (0 in this example). The call should become visible in the internal Queue and the call can be answered.

3. From an external terminal, make an incoming call over ISDN or SIP to the external Queue (8950 in this example). The call should become visible in the external Queue and the call can be answered.

4. From a UNIVERGE 3C terminal make an internal call to the operator. From the operator client answer the call and then click the Park button to park the call. Verify that the call is placed into the park Queue and also verify that the call can be retrieved from the park Queue again.

5. (*Optional Operator Fallback test – see Appendix One*) From an external terminal, make an incoming call over ISDN or SIP to an internal UNIVERGE 3C number that is not answering. After the time out set in UNIVERGE 3C, the call should be forwarded to the fallback Queue of the operator. Verify that the call can be answered.

6. (*Optional Operator Fallback test – see Appendix One*) From an external terminal, make an incoming call over ISDN or SIP to a non-existing internal number. The call should end up at the operator fallback Queue. Verify that the call can be answered.

7. (*Optional Operator Fallback test – see Appendix One*) Perform tests 5 and 6 by making the call from an internal UNIVERGE 3C station. Note that the call should not end up at the operator fallback Queue (fall back should only work for external calls).

24.6.3. Verify VMP IVR lines

Make sure a Starter Line is configured for Prompt Recording Access in BCT.

1. From a UNIVERGE 3C terminal make an internal call to the Prompt Recording Access Starter Line (8922 in this example). A prompt should be heard and in the display of the calling terminal the connected party should be shown as a VMP Line (8910, 8911, 8912, or 8913 in this example).

2. Hang up the call and repeat the test. Again the prompt should be heard and the next VMP line number should be shown. For example, if the previous call displayed 8910, then this call should display 8911.

3. Repeat this test until all of the VMP lines have been accessed and confirm a prompt can be heard on all lines.

24.7. Appendix N-7 - Troubleshooting

Problem: My users do not appear in the BCT company directory

Solution: BCT only considerers a user to be a valid user if the user has full line rights to the station and the user should have a preferred extension assigned

Problem: Some users can call Contact Center or Operator starter lines but others cannot

Solution: Take care that when multiple zones are applied, the zones must have a trust relationship

Problem: My VMP lines do not appear in the configuration wizard and/or BCT Supervisor Dashboard

Solution: VMP lines must be configured in a Round Robin Group, otherwise BCT will not detect then as possible VMP lines

Problem: BCT cannot establish a connection with UNIVERGE 3C – synchronization failure

Solution:

Make sure the servers can ping each other, if necessary enable file and printer sharing exceptions in firewalls to achieve this.

Verify the BCT connection IP port matches the webservice IP port of UNIVERGE 3C (check webservices.xml file on the UNIVERGE 3C server).

Verify if the credentials of the CTI user are entered correctly, in case of doubt, try to logon to the domain using the CTIuser account, if this fails chances are the credentials are incorrect, in that case contact your IT system administrator

Problem: BCT Contact Center does not respond to IVR DTMF input keys

Solution: Check that in UNIVERGE 3C>system properties>media streams tab the DTMF digit payload type is set to 101

Problem: Operator client cannot break in on a call, but the operator terminal can

Solution: Check that the CTIuser account has supervision rights to the address group which is used for the UNIVERGE 3C barge-monitor feature

Problem: VMP line does not answer calls from C-link trunk

Solution: The 3C C-link trunk only supports only 20 msec of G711. Not all public trunks can do this. The work around is using G729 20 msec. Add therefore G729 as Codec for VMP in the BCT Configuration tab Media settings.

Problem: An error message is given when a BCT user with a DECT phone setup a call via the BCT client

When using 3C 8.6.1 or higher, the default setting for IP-DECT phones is to use Out-of-dialog-refer (OOD).
If old DECT sets are used in this environment (not supporting auto-answer on make-call) or auto-answer on make-call is disabled for all terminals in the DECT system (distinctive ringing setting), this will give an error message when the ringing DECT phone is not answered within 5 seconds.

Solution: For all DECT terminals not supporting the auto-answer on make-call function, set Click-to-dial in the related 3C SIP user agent profile to value "intercom-call". When the DECT system has disabled auto-answer on make-call for all terminals, disable OOD in all 3C DECT user agent profiles and set Click-to-dial to value "intercom-call".

24.8. Appendix N-8 – Service conditions

24.8.1. General service conditions

1. VMP Lines, Operator Numbers (internal, external, failover, park), and Contact Center Numbers (pilots, agent logon, messagebox access, prompt recording) must be assigned in the primary UNIVERGE 3C server. They cannot be distributed over a multi UNIVERGE 3C server system.

25. Appendix O – NEC REPORTING PRINT SPOOLER

25.1. Introduction

The purpose of the Reporting Print Spooler is to enable printing of scheduled reports to a printer connected to the BCT server, without having to keep a BCT Supervisor Dashboard client open.

Normally, usage of Reporting Print Spooler does not require manual interaction. The flow of data is described below:

1. The user defines a scheduled report (output on a printer device) in the BCT Supervisor Dashboard application. See BCT Supervisor Guide.

2. At the scheduled time, the BCT server generates the report to a file on the BCT server. By default, these are stored in C:\NEC\Data Files\Reporting PrintQueue folder.

3. The Reporting Print Spooler periodically reads all the generated report files and queues them to the printer, via the *Windows Print Spooler Service*. Queued reports are shown in the Report Print Spooler application.

Important: *To be able to print scheduled reports, you must keep a Windows account logged-on to the BCT Server. The printer has to be installed for this Windows account.*

NEC Reporting Print Spooler is configured to start automatically upon logon.

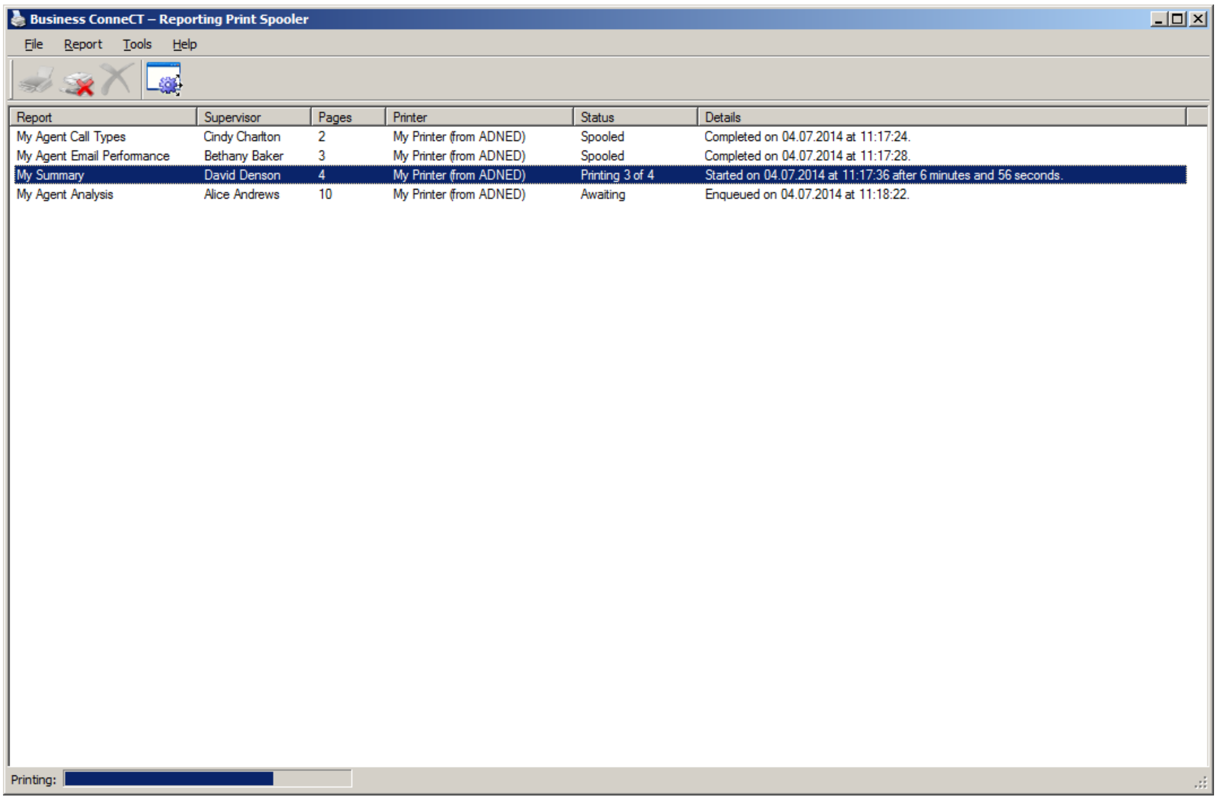
Note: *The report files are not deleted from the disk until the disk space they occupy reaches a configurable limit. The names of the report files have no meaning other than a unique identifier.*

25.2. Using NEC Reporting Print Spooler

To verify the status of the reports queued for printing, you need to open the Report Print Spooler user interface:

1. Double-click the Business ConneCT – Reporting Print Spooler icon in the Windows notification area.

2. The main application screen opens, as pictured in [Figure 25-1 NEC Reporting Print Spooler user interface](#).



Report	Supervisor	Pages	Printer	Status	Details
My Agent Call Types	Cindy Charlton	2	My Printer (from ADNED)	Spooled	Completed on 04.07.2014 at 11:17:24.
My Agent Email Performance	Bethany Baker	3	My Printer (from ADNED)	Spooled	Completed on 04.07.2014 at 11:17:28.
My Summary	David Denson	4	My Printer (from ADNED)	Printing 3 of 4	Started on 04.07.2014 at 11:17:36 after 6 minutes and 56 seconds.
My Agent Analysis	Alice Andrews	10	My Printer (from ADNED)	Awaiting	Enqueued on 04.07.2014 at 11:18:22.

Figure 25-1 NEC Reporting Print Spooler user interface

The user interface displays a list of reports which scheduled for printing, and their current status.

The following information is available in the list:

Report Name of the report for which the print task is created.

Supervisor Name of the supervisor that scheduled the report.

Pages The total number of pages to be sent to the Windows Print Spooler for printing.

Printer The name of the printer to be used for the current task.

Status Status for the current print job, see [25.2.1 Report printing statuses](#).

Details Last activity related to this print task.

To cancel printing of a report:

1. In the Reporting Print Spooler’s list, right-click a report currently being spooled and choose **Cancel**. Or, select the report and choose **Report > Cancel** from the menu.

2. The report will change status to Canceled.

It is possible to re-print reports which were already sent to the printer, or print reports which where previously canceled. This option is especially useful when e.g. printer ran out of toner overnight and printing failed.

To print again a report, do the following:

1. In the Reporting Print Spooler's list, right-click a report and choose **Print**.
   Or, select the report and select **Report > Print** from the menu.

2. The report will change status to Pending and will be sent again to the printer.

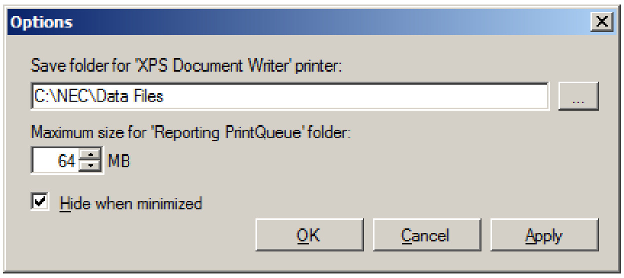
25.2.1. Report printing statuses

Table below shows a complete list of report print job statuses, their meaning, and the manual actions that are available via toolbar/context menu.

Status	**Description**	**Allowed actions**
Awaiting	Printing job is queued and will be automatically spooled to the printer.	-
Manual	Printing job is not queued. It can be deleted or manually scheduled for print.	Print, Delete
Pending	Printing job is queued, after being manually rescheduled for printing.	-
Spooling	Printing job is currently spooling to the Windows Print Spooler Service.	Cancel
Spooled	Printing job was successfully spooled.	Delete
Canceled	Printing job was canceled by the user. You can delete it, or re-schedule it for printing.	Print, Delete
Missing printer	Printing job failed because printer is no longer available in the system.	Print, Delete
Not configured	Printing job was sent to an XPS printer, but Report Print Spooler is not configured. See 25.2.2 Options.	Print, Delete
File not found	Printing job failed because the report file is no longer on disk. This may occur if you manually deleted files from the BCT Server.	Delete
Error	The job print action finished with errors. The Details column may provide additional information.	Print, Delete

25.2.2. Options

To configure options for Reporting Print Spooler, use **Tools > Options** from the menu. The Options screen is presented in Figure 25-2 Reporting Print Spooler options.



Save folder for 'XPS Document Writer' printer: C:\NEC\Data Files

Maximum size for 'Reporting PrintQueue' folder: 64 MB

☑ Hide when minimized

Figure 25-2 Reporting Print Spooler options

Save folder for XPS Document Writer printer

Path to a local folder where *.xps files are saved.

This is only required when printing to a "Microsoft XPS Document Writer". Otherwise, you may leave it empty.

Note: *If this path is left empty and a user tries to print reports to a "Microsoft XPS Document Writer" virtual printer that may be installed on the server, those reports will show up as Not configured in the list. See 25.2.1 Report printing statuses.*

Maximum size for 'Reporting PrintQueue' folder

Specifies the maximum size, in MB, of report print jobs to be kept in the C:\NEC\Data Files\Reporting PrintQueue. When this size is exceeded, the oldest files are removed.

Hide when minimized

Indicates that the application should be removed from the Windows task bar while minized. By default, this is checked.

26. Appendix P – SERVER MANAGER

26.1. Introduction

The *Server Manager* application is primarily intended to assist in BCT migration scenarios (e.g. migrating to a new Windows operating system or towards a virtualized environment). It offers support to backup and restore BCT configuration data, i.e. database as well as settings (e.g. configuration file settings). Further it also offers the option to change the SQL password of the SQL account used by the BCT services/applications.

The *Server Manager* application offers the following functionality:

- “Backup Configuration” from BCT 5.x and higher
- “Restore Configuration” on BCT 7.x and higher
- “Configure SQL Password” to maintain BCT services SQL account
- Setting secure port bindings

Notes:

- *Backup and restore of SQL ‘United’ database is included when database is on the BCT server. For BCT systems using a remote SQL server please refer to chapter* ***26.3 Remote SQL Server****.*

- *Backup (and restore) configuration aspects* ***NOT*** *covered are:*
  - Current active diagnostics trace-level-settings
  - Own saved diagnostics template files
  - Aranea settings, such as customized mappings in VBScript files
  - PMS Connector data files

- *Backup from BCT systems using Dialogic boards for IVR are* ***NOT*** *supported*

- *For a smooth migration scenario it is strongly recommended to restore to a server with the same name as the old one! Restoring to a new server with a different name will require an uninstall/re-install of all Desktop Clients, Contact Center Clients and Soft Wallboard Clients.*

- *When a restore is done as part of a migration scenario that requires a new BCT license on the targeted BCT server at the moment the restore has finished load the new BCT license before the scheduled reboot.*

- *Application requires .NET Framework 4.5.2 (which should be installed on BCT 7.10.x and later systems).*
  In case of BCT systems before BCT 7.10.x a recent .NET Framework must be installed manually.
  The .NET Framework 4.8 is available on the BCT DVD via autorun.exe installation menu.

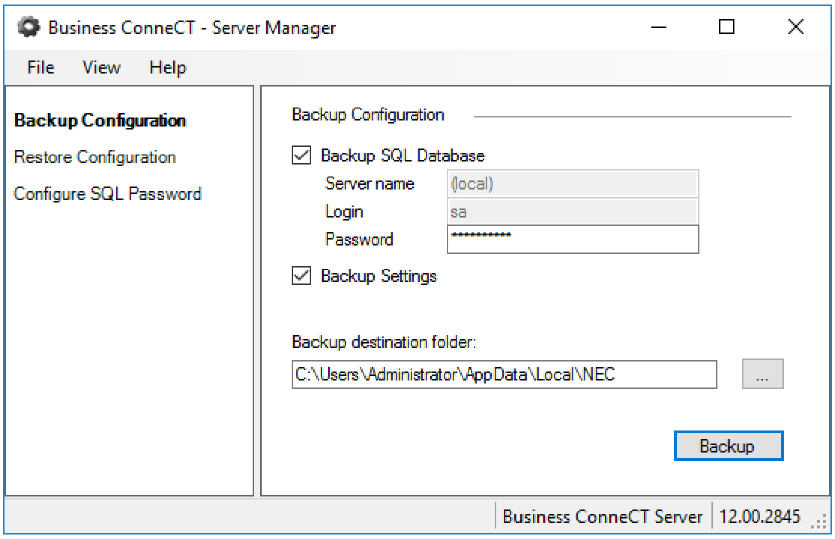
To use the *Server Manager* application on BCT 5.x server or BCT 6.x server systems, start ‘ServerManager.exe’ from the BCT DVD. It can be found in folder “D:\Business ConneCT Resources\Configuration Support\Server Manager” (where D is the drive letter of your DVD drive).

To use the *Server Manager* application (available since BCT 7.x) start the Server Manager via **Start > Programs > Business ConneCT > Tools > Server Manager**.

26.2. Usage Guidelines

In the next sub-chapters some additional usage information can be found for each offered functionality.

26.2.1. Backup Configuration



Backup Configuration

☑ Backup SQL Database

Server name: (local)

Login: sa

Password: ***********

☑ Backup Settings

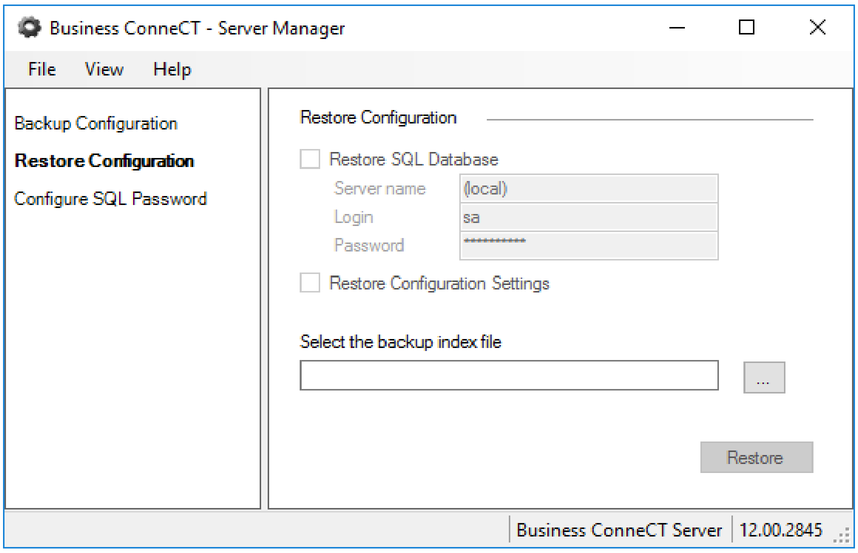
Backup destination folder: C:\Users\Administrator\AppData\Local\NEC

Figure 26-1 Server Manager - Backup Configuration window

In the backup destination folder, the following information will be saved:

- The backup data. This consists of an .inx backup index file plus ZIP files for database and settings
- The backup task-related log file that is created during backup. This log file can also be accessed also via menu **View > Log File**.

26.2.2. Restore Configuration



Restore Configuration

☐ Restore SQL Database

Server name: (local)

Login: sa

Password: ***********

☐ Restore Configuration Settings

Select the backup index file

Figure 26-2 Server Manager - Restore Configuration window

To restore a backed-up configuration, do the following:

1. Select the .inx backup index file

2. Optionally, deselect one of the ‘Restore’ checkboxes in case specific restore is not wanted.

3. Click **Restore**. The restore task-specific log is created in same folders were backup index file is located and can be accessed via menu **View > Log File**.

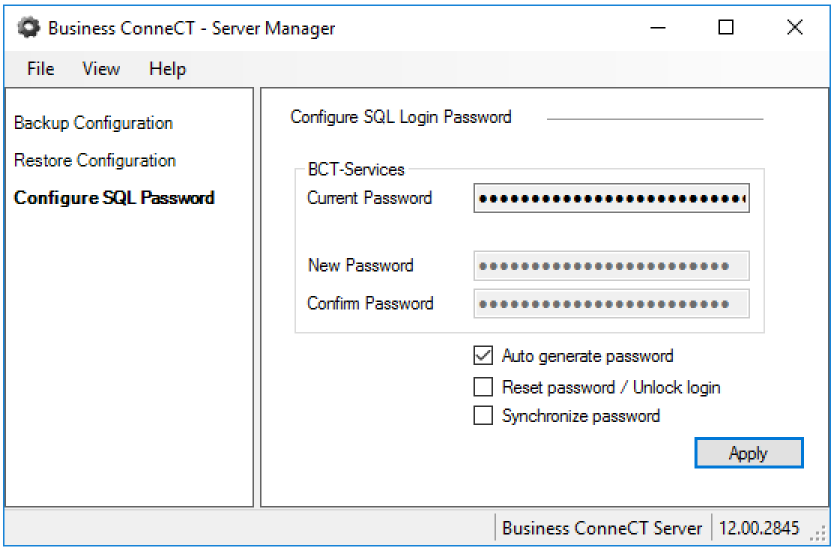
26.2.3. Configure SQL Password

The Business ConneCT system typically uses a SQL login named ‘BCT-Services’ to access the ‘United’ database on the SQL server. The password for this ‘BCT-Services’ is normally (when default installation was done) an auto-generated password and saved (encrypted) in XML configuration file “C:\Program Files (x86)\Common Files\NEC\Configuration\DatabaseConfiguration.xml”.

It is obvious that this password value must be in sync with actual SQL server password for the ‘BCT-Services’ SQL login. In order to keep these values identical it is strongly recommended to configure (maintain) the password using the ‘Server Manager’ application.
For normal scenario the password can be changed as shown in screen below.

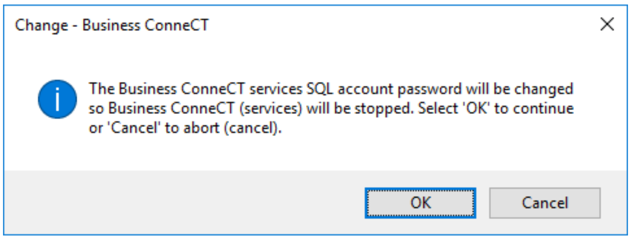
Note:

- *In case Business ConneCT is installed with custom database name the SQL login account used will be named ‘BCT-[databasename]’*



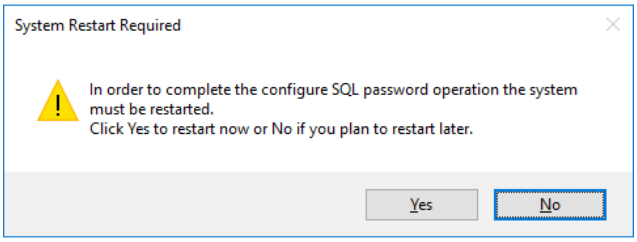
- Have ‘Auto generate password’ checkbox checked for an auto-generated password or
- Have ‘Auto generate password’ checkbox unchecked to manually enter a password

When the **Apply** button is clicked the next message is shown:


Change - Business ConneCT

The Business ConneCT services SQL account password will be changed so Business ConneCT (services) will be stopped. Select 'OK' to continue or 'Cancel' to abort (cancel).

When **OK** clicked the password change will be effectuated and when successfully finished next 'System Restart Required' message is shown. Click **Yes** to initiate the restart.



System Restart Required

In order to complete the configure SQL password operation the system must be restarted.
Click Yes to restart now or No if you plan to restart later.

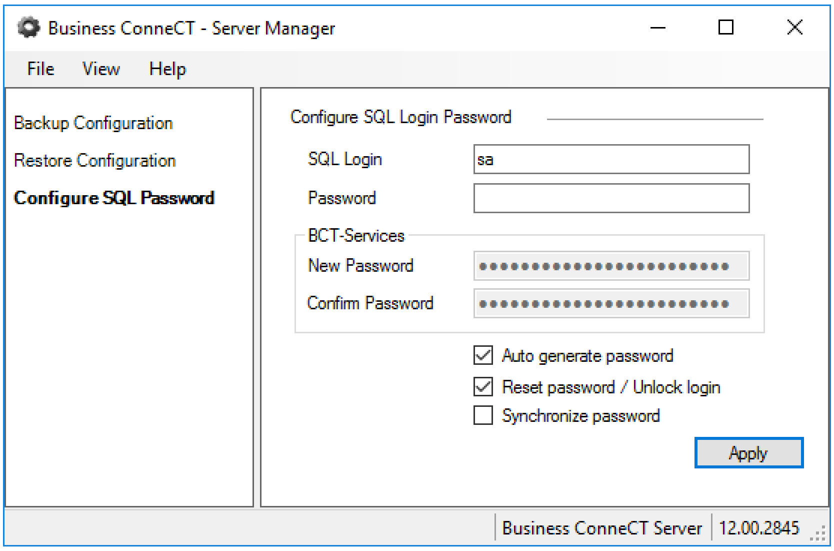
You might be confronted with situations were the change password operation will fail like:

- SQL login account is locked out due to too many failed logon attempts
- SQL login password is changed with SQL Server Management Studio

In order to recover from these situations next options are included:

- Reset password / Unlock login
- Synchronize password

When "Reset password / Unlock login" checkbox is checked the screen below is shown:



SQL Login: sa

Password:

BCT-Services

New Password: ••••••••••••••••••••••••

Confirm Password: ••••••••••••••••••••••••

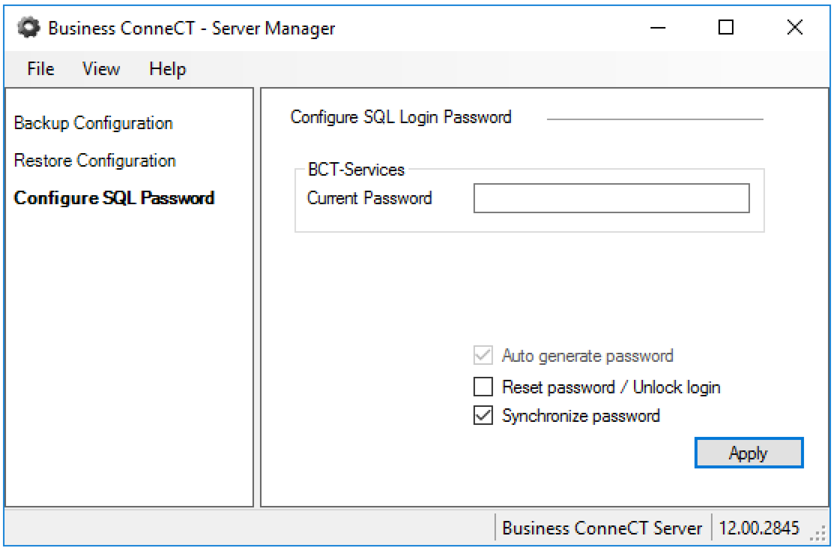
☑ Auto generate password

☑ Reset password / Unlock login

☐ Synchronize password

This recovery mode will allow you to reset the SQL login password and unlock the SQL login (when applicable). So the SQL password is changed (unlocked) on the SQL server and when succeeded the password is saved (encrypted) in the XML configuration file.

When “Synchronize password” checkbox is checked (and “Reset password / Unlock login” checkbox is unchecked) the screen below is shown:



Configure SQL Login Password

BCT-Services

Current Password

☑ Auto generate password

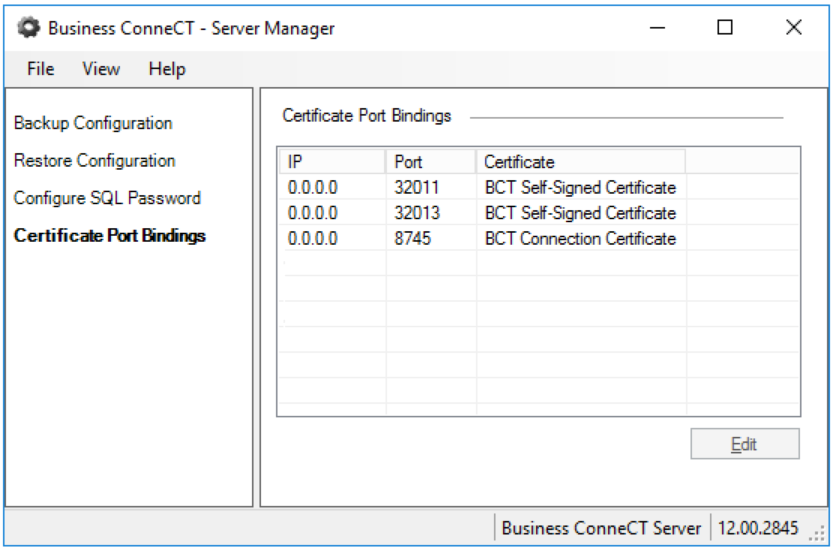
□ Reset password / Unlock login

☑ Synchronize password

This recovery mode will allow you to synchronize the SQL login password. So for situations where the SQL login password is known (e.g. accidentally changed on SQL server) and you want the password synchronized and saved (encrypted) in the XML configuration file.

26.2.4. Certificate Port Bindings

To modify or repair Secure Ports Bindings, start the Server Manager and select “Certificate Port Bindings”. The current bindings are shown

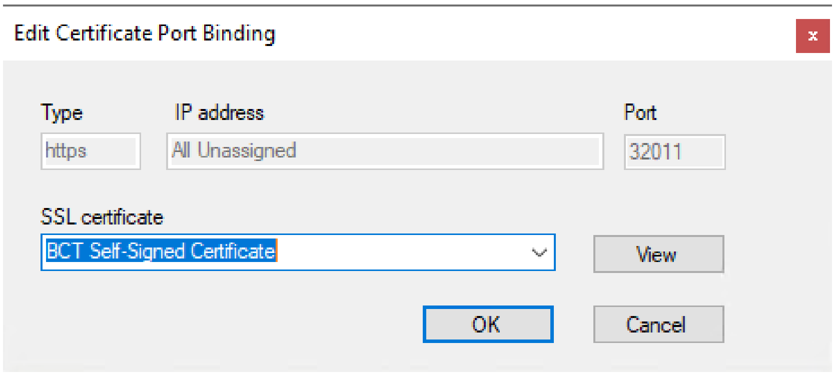


Certificate Port Bindings

IP	Port	Certificate
0.0.0.0	32011	BCT Self-Signed Certificate
0.0.0.0	32013	BCT Self-Signed Certificate
0.0.0.0	8745	BCT Connection Certificate

Figure 26-3 Server Manager – Certificate Port Bindings window

Select the binding line to be adapted and press Edit, the next window appears:



Type: https

IP address: All Unassigned

Port: 32011

SSL certificate: BCT Self-Signed Certificate

Figure 26-4 Server Manager – Certificate Port Bindings edit window

In the dropdown, select the appropriate certificate and press the OK button to apply the change.

26.3. Remote SQL Server

When the BCT server is using a remote SQL server the backup and restore for the ‘United’ database is skipped.

Please use the example scenario below for migration, where the following assumptions are made:

- you have a current operational BCT server named “BCTSERVERW2K3”
- your BCT server uses a ‘United’ database on the default SQL instance named “BCTSERVERSQL\MSSQLSERVER” on a remote SQL server named “BCTSERVERSQL”
- you migrate to a new BCT server with server name “BCTSERVERVIRTUAL”

1. Use SQL Management Studio manually to make a full backup of the current ‘United’ database.

2. Use SQL Server Installation to create a new named SQL instance (e.g. “BCTSERVERSQL\MSSQLBCT”) on the remote SQL server “BCTSERVERSQL”.

3. On the new “BCTSERVERVIRTUAL” server install a new BCT 8.x server and use the new named instance (i.e. “BCTSQLSERVER\MSSQLBCT”) to create the new ‘United’ database. This is to prevent that it will interfere with you current operational BCT server

4. Use the *Server Manager* application to backup the configuration settings of the BCT server “BCTSERVERW2K3”.

5. Use the *Server Manager* application to restore the backed up BCT server configuration settings on the new BCT server “BCTSERVERVIRTUAL”.

6. Use SQL Management Studio manually to restore the backup made of the ‘United’ database on the new named “BCTSQLSERVER\MSSQLBCT” SQL instance.

7. Run *Database Maintenance* application (i.e. ‘Installer.Database.exe’ from “C:\Program Files (x86)\Common Files\NEC\Database SQL Scripts”) and after having opened the connection initiate an ‘Upgrade Database’ action. Note that the *Database Maintenance* application is already aware of the new named instance “BCTSQLSERVER\MSSQLBCT”.

27. Appendix Q – APPLYING QOS TO IVR LINES (VMP)

Quality of Service (QoS) for VMP (IVR) can be applied by means of a *Windows Group Policy*. Using the Group Policy Editor you can create a QoS-rule to the VMP-Service so that you can manage your VoIP network traffic giving it higher priority over normal data network traffic.

Important: *All your network equipment (routers) must support QoS. If any network device between the endpoints (VMP and e.g. IP-Telephone) does not support QoS, then traffic management stops from that point.*

How to apply QoS-rule:

1. Start the **Group Policy Editor**.
   You can open the Local Group Policy Editor by using the command line or by using the Microsoft Management Console (MMC):

- Via command-line:
  Click **Start** , type *gpedit.msc* in the **Start Search** box, and then press **ENTER**

- Via MMC as snap-in:

- Open MMC. (Click **Start** , click in the **Start Search** box, type *mmc* , and then press **ENTER**)
- On the **File** menu, click **Add/Remove Snap-in**
- In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**
- In the **Select Group Policy Object** dialog box, click **Browse**
- Click **This computer** to edit the Local Group Policy object
- Click **Finish**

2. Go to Computer Configuration and proceed to Windows Settings

3. Right-click on **Policy-based QoS** -> **Advanced QoS Settings** -> **DSCP Marking Override**
   And make sure that *'Allowed'* is enabled and checked and press **OK**.
   This makes sure your settings won't overrule DSCP request from other applications.

4. Now create new rule by right-click on **Policy-based QoS** -> **Create new policy…**

- Name it (e.g. VMP QoS) and give it the desired **DSCP** value (e.g. 46) and press **Next**.
- Now have this rule only apply to VMP:
  Select **Only applications with…** and enter *VmpService.WinService.exe*
- Keep the defaults for source/destination IP addresses (=any) and press **Next**.
- Select '**UDP'** to apply this QoS rule (the VoIP media stream uses UDP protocol).
- Finish.

How to verify that a QoS rule is applied:

1. Use e.g. Wireshark to capture network traffic to capture some media-stream.

2. When checking the DSCP-field (in IP-header), it should contain the configured DSCP-value.

28. Appendix R – Dongle Usage (Asian Market Only)

28.1. Introduction

This appendix contains information for BCT servers using a hardware dongle for licensing which only is applicable for the Asian market.

28.2. Activate BCT Licenses

1. Start the License Manager via Start-Menu > Programs > Business ConneCT > Tools > License Manager. The next next window will appear:

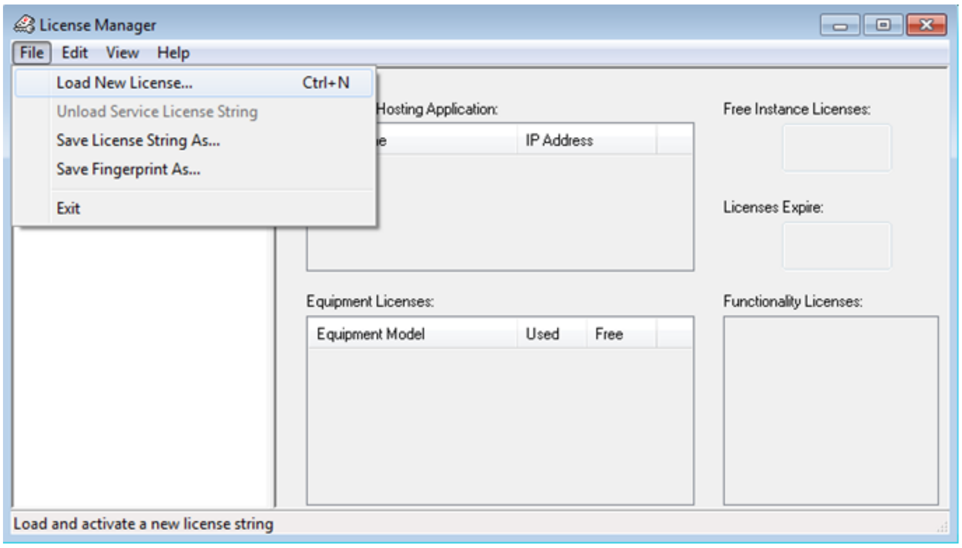


Figure 28-1 License Manager Main Window

2. Load the license string via File > Load New License. The next window will appear:

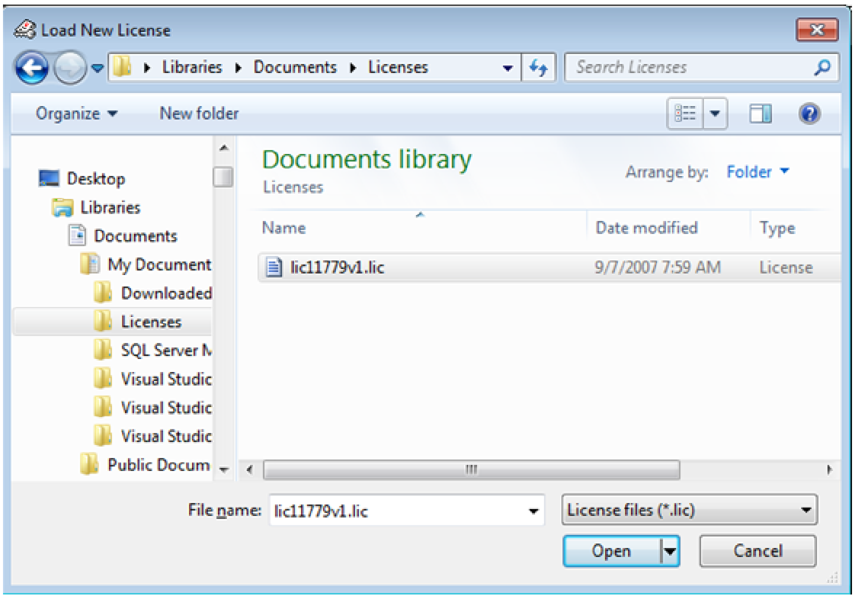


Figure 28-2 License Manager Load New License Window

3. Close the License Manager application

28.3. Virtualized Server Environment

BCT server can run in a virtualized server environment. However USB is not always supported in virtual environments so you will need to have some kind of USB over IP solution in your network. BCT has a solution in the form of remote USB dongle support. You need to have a PC in your network that will function as a remote USB hub.

1. Install the dongle driver on the remote dongle PC from the BCT DVD (D: in example)
   - Run D:\Business ConneCT 12.00\Server\Prerequisites\Bin\Sentinel Protection Installer 7.6.9.exe
2. Connect the BCT USB dongle to remote dongle PC.
3. Configure the BCT server to use the remote dongle.
   - Open the License Manager via Start-Menu > Programs > Business ConneCT > Tools > License Manager
   - Select the menu Edit > Remote Dongle
   - Fill in the IP-address of the remote dongle PC (where dongle is physically connected).
   - Confirm with OK
   - The system will ask you to reboot (mandatory to get this working).
4. After reboot start the License Manager and load the license file.

NOTE:
When using the BCT dongle as a remote dongle on a remote dongle PC it will require UDP port 6001 to be open (i.e. not blocked by a firewall) on the remote dongle PC itself.

29. Appendix S – Customizing email notification

If configured the user has the possibility to receive emails as notification for voicemails or missed calls.

The notification emails make use of the templates installed in data folder of the BCT server, by default in C:\NEC\Data Files\UCS-Module. The templates are html files with the name starting with “VoicemailTemplate_“or “MissedCallTemplate_” followed by the culture name (e.g. VoicemailTemplate_en-US.htm).

The notification email will attempt to use the language configured for the user receiving the notification, providing this language is present within the templates.

There are already a few templates installed by default, including English. If the template for the language used by the defined users is not present within the installed templates, it can be easily added. To add a new template file follow the following steps:

1. Copy - Paste the existing English template file into the same folder.
2. Change its name according to the user language you want to use (e.g. MissedCallTemplate_de-DE.htm)
3. Modify its content by translating the English text to your language. In order to figure out which text to be changed, open the file using an Internet browser. All visible text can be translated into your language. Do not translate the text between ## (e.g. #CallerPhone#) and to not translate the html related keywords. Translate only the text visible when opening the html template file with the Internet Browser.

One can only create templates for the languages supported by the system. The culture strings accepted to be added to the template file name are: ar-AE (Arabic), ca-ES (Catalan), zh-CN (Chinese), da-DK (Danish), nl-NL (Dutch), en-UK (English, UK), en-US (English, US), fr-FR (French), de-DE (German), el-GR (Greek), it-IT (Italian), ja-JP (Japanese), nb-NO (Norwegian, Bokmal), nn-NO (Norwegian, Nynorsk), pl-PL (Polish), pt-BR (Portuguese, Brasil), pt-PT (Portuguese, Portugal), ru-RU (Russian), es-ES (Spanish, Spain), sv-SE (Swedish), tr-TR (Turkish).

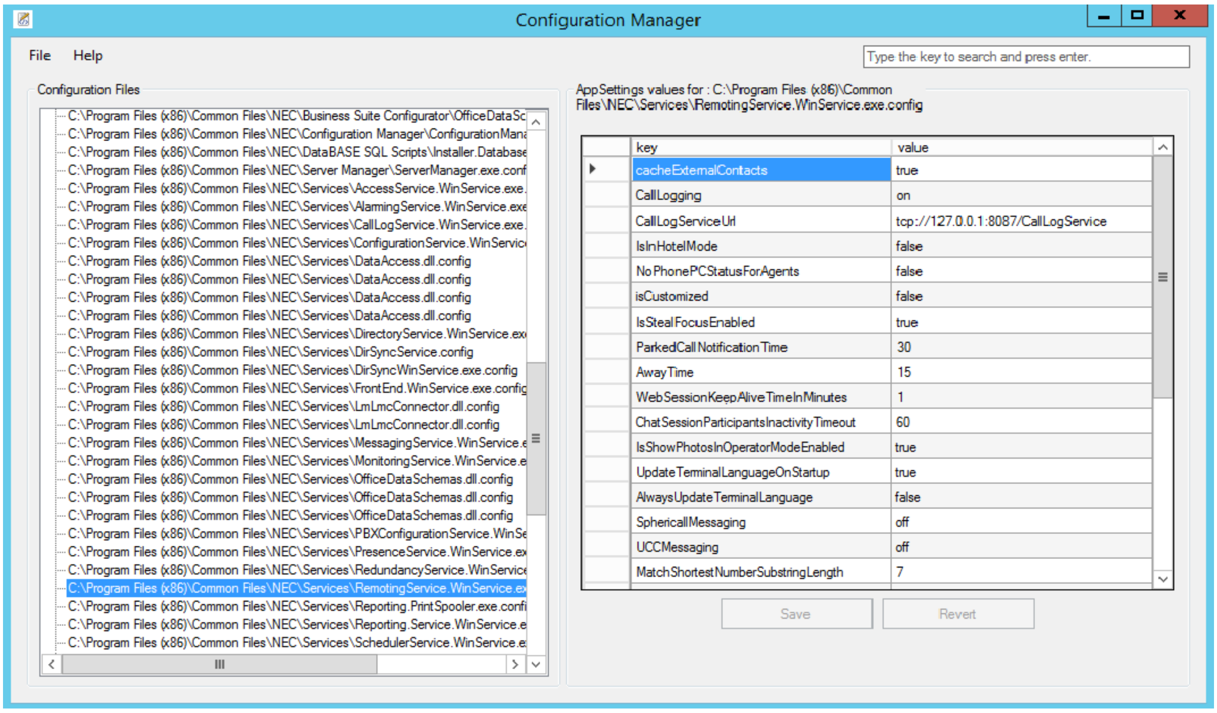
When the required template is missing the system will use the English template by default.

The html styles and colors of the template file can be changed as well to get a fully customized notification email.

30. Appendix T - Configuration Manager

To enable functionality or change behavior for Business ConneCT it is sometimes required to modify settings in configuration files. To assist with modifing the (app setttings part) configuration files the tool Configuration Manager can be used. This tool is available on the BCT server via Start/Programs/Business Connect/Tools.

When startup the tool all the BCT configuration files are loaded and displayed in the left pane of the tool. When doubleclicking on a configuration file then the right pane reveals all the keys (in the App setting) and their current values.



```
C:\Program Files (x86)\Common Files\NEC\Business Suite Configurator\OfficeDataSc
C:\Program Files (x86)\Common Files\NEC\Configuration Manager\ConfigurationMana
C:\Program Files (x86)\Common Files\NEC\DataBASE SQL Scripts\Installer.Database
C:\Program Files (x86)\Common Files\NEC\Server Manager\ServerManager.exe.conf
C:\Program Files (x86)\Common Files\NEC\Services\AccessService.WinService.exe.
C:\Program Files (x86)\Common Files\NEC\Services\AlarmingService.WinService.exe
C:\Program Files (x86)\Common Files\NEC\Services\CallLogService.WinService.exe.
C:\Program Files (x86)\Common Files\NEC\Services\ConfigurationService.WinServic
C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\DataAccess.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\DirectoryService.WinService.ex
C:\Program Files (x86)\Common Files\NEC\Services\DirSyncService.config
C:\Program Files (x86)\Common Files\NEC\Services\DirSyncWinService.exe.config
C:\Program Files (x86)\Common Files\NEC\Services\FrontEnd.WinService.exe.config
C:\Program Files (x86)\Common Files\NEC\Services\LmLmcConnector.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\LmLmcConnector.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\MessagingService.WinService.e
C:\Program Files (x86)\Common Files\NEC\Services\MonitoringService.WinService.e
C:\Program Files (x86)\Common Files\NEC\Services\OfficeDataSchemas.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\OfficeDataSchemas.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\OfficeDataSchemas.dll.config
C:\Program Files (x86)\Common Files\NEC\Services\PBXConfigurationService.WinSe
C:\Program Files (x86)\Common Files\NEC\Services\PresenceService.WinService.ex
C:\Program Files (x86)\Common Files\NEC\Services\RedundancyService.WinService
C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.ex
C:\Program Files (x86)\Common Files\NEC\Services\Reporting.PrintSpooler.exe.confi
C:\Program Files (x86)\Common Files\NEC\Services\Reporting.Service.WinService.e
C:\Program Files (x86)\Common Files\NEC\Services\SchedulerService.WinService.e
```

AppSettings values for : C:\Program Files (x86)\Common Files\NEC\Services\RemotingService.WinService.exe.config

key	value
cacheExternalContacts	true
CallLogging	on
CallLogServiceUrl	tcp://127.0.0.1:8087/CallLogService
IsInHotelMode	false
NoPhonePCStatusForAgents	false
isCustomized	false
IsStealFocusEnabled	true
ParkedCallNotificationTime	30
AwayTime	15
WebSessionKeepAliveTimeInMinutes	1
ChatSessionParticipantsInactivityTimeout	60
IsShowPhotosInOperatorModeEnabled	true
UpdateTerminalLanguageOnStartup	true
AlwaysUpdateTerminalLanguage	false
SphericallMessaging	off
UCCMessaging	off
MatchShortestNumberSubstringLength	7

To change the value simply click on the value and change the value. By pressing button Save the value is saved in the configuration file. Pressing button Revert will undo any changes made to the values.

It is also possible to search for a key through all configuration files. Enter the key or part of the key in the Search field and press enter. The right pane will reveal all the configuration files where the key is found. Select the required file and right pane will show all the key’s (of the App setting), including the key that was searched for.

The Configuration Manager only allows editing existing keys. To add or remove keys an external text file editor must be used. Right mouse click on a config file, choose Open or Open With to open the configuration file with an external file editor like Notepad.

31. Appendix U – Move extensions to other PBX

There are three main scenarios concerning the move of extensions to another PBX:

1. Move extensions to another unit in an iS3000 IMP network.
2. Move extensions between PBXs which are already defined in BCT.
3. Add another PBX to BCT and move extensions to the new PBX.

The first scenario is already covered by the synchronization functionality – an iS3000 IMP network is synchronized as a single PBX, synchronization can handle extensions moved to another unit. See 8.1.5 Connection to PBX.

This appendix covers the other two scenarios.

31.1. Introduction: the move session

Moving extensions to another PBX (except for scenario 1 described in the previous section) can only be done during a move session.

A move session can be started and closed from System Settings. During a move session the PBX synchronizations work in a different mode. The differences are listed in the table below.

Synchronization in normal mode	**Synchronization during move session**
When extension found in another PBX, a 'duplicate extension' error is given.	When extension found in another PBX, the extension is moved to the PBX for which the synchronization is running now.
When an extension was not found anymore after synchronization of the PBX, the extension is deleted. When the extension was on 3C, the user of the extension is deleted, otherwise the user will be moved to the dummy extension ##**##.	When an extension was not found anymore after synchronization of the PBX, the extension is parked on a temporary PBX. Think of this temporary PBX as a kind of 'garbage bin' where the extension is stored until the end of the move session – or until the extension is found during synchronization of another PBX in the same move session. When the extension is still on the temporary PBX when the move session is closed, it will be deleted. When the extension originally was on 3C, the user of the extension is deleted, otherwise the user will be moved to the dummy extension ##**##.

During a move session the PBXs can be synchronized in any order.

The global scenario for a move scenario is as follows:

1. Isolate BCT from changes in PBXs, e.g. stop all synchronizations.
2. Do all required work on the PBXs, like (re-)configure the PBXs and/or add (a) new PBX(s).
3. Open a move session in BCT (System Settings).
4. Manually synchronize the PBXs.
5. Close the move session.

6. Do some afterwork when required.

Detailed scenarios are described in the next sections.

31.1.1. Restrictions

This feature has the following restrictions:

1. Move extensions is not supported for configurations with Open Number Scheme.

2. Most properties of an extension and the related user will be kept over a move, like roles, call logs, forwardings with active presence profile, etc. However depending on the different characteristics of the PBX where the extension was originally assigned and the new PBX, some properties might be lost.

The following properties might require adaptations afterwards:

- 3C setting ‘Allow modification of address centric users’ is forced to ‘on’ when an extension is moved from another PBX type to the 3C PBX. You might want to switch it ‘off’ after the move.
- When VMP lines were removed from a PBX, re-assign the VMP lines in the proper PBX. Do **NOT** forget to also save/adapt the media ports configuration.
- When Routing points were moved from a PBX, re-assign the Routing points in the proper PBX.
- Call forwarding settings of extensions may be lost, e.g. when there was already a different call forwarding for this extension in the target PBX, or when the origin PBX supported different forwardings for internal and external calls, and the target PBX does not have this feature. When the move session is closed, BCT will set the call forwarding as configured in the user’s current profile.
- Group assignments will be lost when a group member is moved to another PBX while the group is not moved.
- DND setting might be lost.
- Twinning setting will be lost.
- SMA setting will be lost.
- Manual terminal type will be lost.
- Call positions of a terminal might be lost.
- Multi-line settings are lost.
- When TieExtension source or slave extension is moved to another PBX type, the TieExtension relation will be lost.

The possible required actions can be derived from the report of the move session that made when the move session is closed.

31.1.2. Move session handling in System Settings

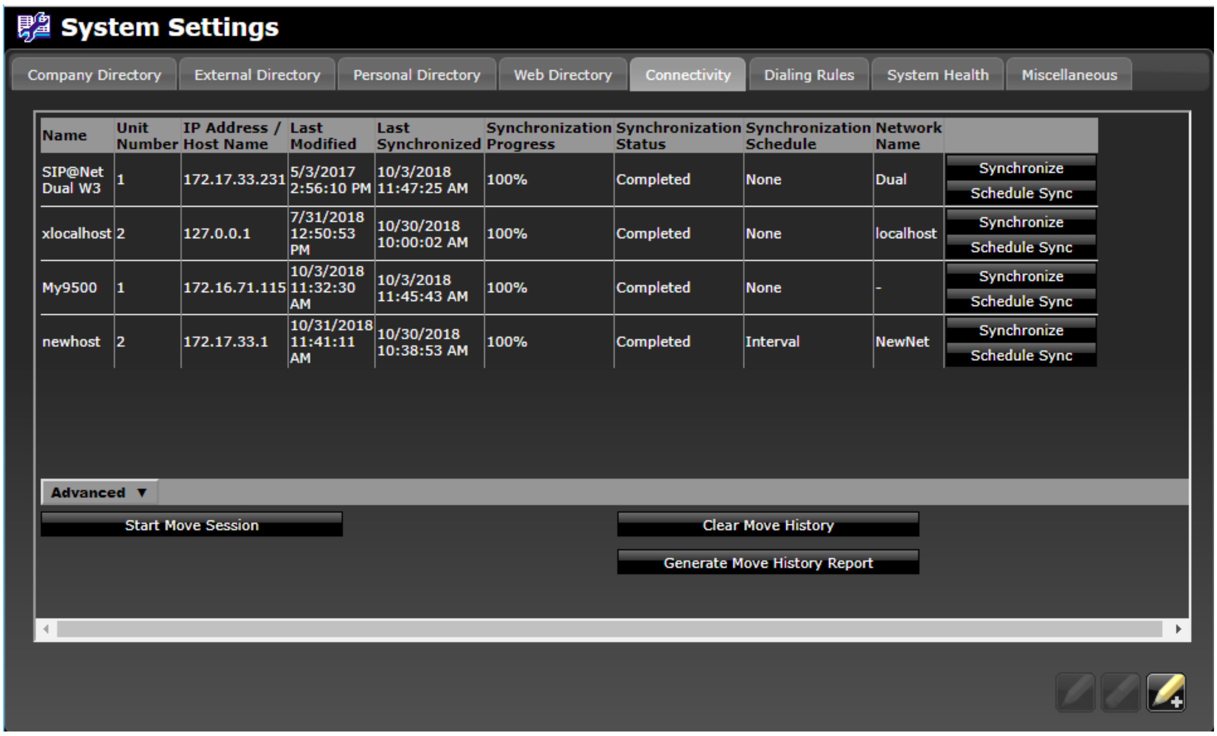
Move sessions can be controlled in the System Settings Connectivity tab.

To show the Advanced section at the bottom of the Connectivity tab, the following key must be added in the configuration file: “C:\Inetpub\wwwroot\DirectoryBrowser\web.config”

```
   <add key=”IsPbxAdvancedSettingsEnabled” value=”true”/>
```

The Advanced section is only shown when there are at least two PBXs defined.

Open the Advanced section to control the move session.



Name	Unit Number	IP Address / Host Name	Last Modified	Last Synchronized	Synchronization Progress	Synchronization Status	Synchronization Schedule	Network Name	
SIP@Net Dual W3	1	172.17.33.231	5/3/2017 2:56:10 PM	10/3/2018 11:47:25 AM	100%	Completed	None	Dual	Synchronize Schedule Sync
xlocalhost	2	127.0.0.1	7/31/2018 12:50:53 PM	10/30/2018 10:00:02 AM	100%	Completed	None	localhost	Synchronize Schedule Sync
My9500	1	172.16.71.115	10/3/2018 11:32:30 AM	10/3/2018 11:45:43 AM	100%	Completed	None	-	Synchronize Schedule Sync
newhost	2	172.17.33.1	10/31/2018 11:41:11 AM	10/30/2018 10:38:53 AM	100%	Completed	Interval	NewNet	Synchronize Schedule Sync

Figure 31-1 Connectivity tab: handle move session

The Advanced section shows three buttons:

- Start/Close Move Session.
  When a new move session is started some other functionality is disabled:
  edit, add or delete a PBX (PBX edit page is read-only),
  edit, add, delete, import or export company directory data.
  When the move session is closed, all functionality is enabled again and a report is generated of the latest move session.
  While a PBX synchronization is in progress the button is disabled.

- Clear Move History.
  The move log data in the database which is used to generate move session reports is cleared.

Note: *When you use move sessions more often it is advised to regularly clear the move history. It might also be required to shrink the transaction log file of the database, see* 10 BACKUP AND DATABASE MAINTENANCE.

- Generate Move History Report.
  A report is generated of all move sessions of which the log data is still available in the database.

At the bottom of the Advanced section a status line will show the result of the latest action and possible additional information like the location of the session report.
Note: all created log files are available in “C:\NEC\Data Files\Move Extension Logging”

31.2. Move extensions between currently assigned PBXs

You follow this scenario mainly to move extensions around on the PBXs which are already known in BCT.

Follow the scenario as below:

1. Database: Make a backup of the database.
2. BCT:
    a. Stop Aranea synchronization.
    b. Disable all scheduled synchronizations.
    c. Switch off redundancy settings when applicable, or at least ensure you are running on the master/primary node and failover is inhibited.
3. PBXs: Re-arrange assignment of extensions.
4. BCT: In the Directory Browser, in the Connectivity tab:
    a. Open the 'Advanced' tab at the bottom of the screen.
    (When you have no Advanced tab you might need to define a key in the web.config file, see above.)
    Start a move session.
    (A temporary PBX named ###### will be created to store 'orphan' extensions.)
    b. Synchronize all involved PBXs.
    PBXs can be synchronized in any order.
    c. After the synchronization has been completed, check that no extensions are left on the temporary PBX, or only those extensions you want to delete: open Directory Browser/Company Directory, select 'Extension' and search for extensions in the temporary PBX.
    Any extension left in the temporary PBX that should be moved to another PBX?
    Configure the extension on the proper PBX and synchronize that PBX again.
    Repeat until all extensions are on the proper PBX.
    d. Under the 'Advanced' tab, close the move session.
    The temporary PBX will be deleted and a report with details about the move session is made available as mentioned at the bottom of the 'Advanced' section.
5. BCT: Investigate the report to find out whether some afterwork is required.
Perform the proper actions.
6. BCT: Restart the functions that were stopped to prepare for the move (as far as required):
    a. Start Aranea synchronization.
    b. Schedule PBX synchronizations.
    c. Configure redundancy for redundant PBXs.

31.3. Move extensions to a new PBX

Main reason to follow this scenario is when you want to replace an existing PBX by a new one.
E.g. when changing to a new PBX type: add a new PBX, move all extensions from the old PBX to the new PBX and delete the old PBX.

To achieve this, follow the following scenario:

1. Database: Make a backup of the database.
2. BCT:
    a. Stop Aranea synchronization.
    b. Disable all scheduled synchronizations.

   c. Switch off redundancy settings when applicable, or at least ensure you are running on the master/primary node and failover is inhibited.

3. PBX: Configure the new PBX including all extensions.
4. BCT: In the Directory Browser, in the Connectivity tab:
   a. **Only add** the new PBX to BCT. You will get a popup with a question whether you want to **synchronize the new PBX; answer 'No'** (**Do not synchronize the new PBX yet)!**
   b. Open the 'Advanced' tab at the bottom of the screen.
      (When you have no Advanced tab you might need to define a key in the web.config file, see above.)
      Start a move session.
      (A temporary PBX named ###### will be created to store 'orphan' extensions.)
   c. Synchronize the new PBX.
   d. After the synchronization has been completed, check that all extensions are moved to the new PBX: open the Directory Browser/Company Directory, select 'Extension' and search for extensions in the old PBX.
      Any extension left in the old PBX that should be moved to the new PBX?
      Configure the extension on the new PBX and synchronize the new PBX again.
      Repeat until all extensions are on the proper PBX.
   e. Under the 'Advanced' tab, close the move session.
      The temporary PBX will be deleted and a report with details about the move session is made available as mentioned at the bottom of the 'Advanced' section.
5. BCT: Investigate the report to find out whether some afterwork is required.
   Perform the proper actions.
6. BCT: Delete old PBX when relevant.
7. BCT: Restart the functions that were stopped to prepare for the move (as far as required):
   a. Start Aranea synchronization.
   b. Schedule PBX synchronizations.
   c. Configure redundancy for redundant PBXs.

32. Appendix V – Exchange and Social Media Proxy Settings

Remoting Service

The NEC Remoting Service can communicate with the Exchange Web Server and with Social Media Providers. By default connection to the Exchange Web Service and Social Media Provider will not go through a proxy server. If the Exchange Web Service or the Social Media Provider can only be accessed from the BCT computer through an internet proxy then you must configure the proxy settings.

On the Business ConneCT server:

- Browse to "C:\Program Files (x86)\Common Files\NEC\Services" and use a text editor (e.g. Notepad) to open the file "RemotingService.WinService.exe.config" and search for section "defaultProxy".

    - To use system default proxy change the proxy section as follows:

      ```
      <defaultProxy>
              <proxy usesystemdefault="True"/>
      </defaultProxy>
      ```

    - To view the system default proxy settings go to
      Control Panel->Internet Options->Connections->LAN Settings

        - To use a custom proxy with a URL change the proxy section as follows (address and port are fictive):

          ```
          <defaultProxy>
                  <proxy usesystemdefault="False"
                          proxyaddress="http://192.168.100.60:8080"/>
          </defaultProxy>
          ```

        - To use a custom proxy with a script change the proxy section as follows (address and script name are fictive):

          ```
          <defaultProxy>
                  <proxy usesystemdefault="False"
                          scriptLocation="http://192.168.100.60/dmz-
                          proxy.pac"/>
          </defaultProxy>
          ```

    - If you have to use a proxy for one server and cannot use it for another server then you have to add a “bypasslist” element.

        - For example if a proxy must be used for the Social Media Provider and the proxy cannot be used for an Exchange Server with IP address 192.168.27.123 then change the defaultProxy section as follows:.

          ```
          <defaultProxy>
                  <proxy usesystemdefault="True"/>
                  <bypasslist>
                  <add address="192\.168\.27\.123" />
                  </bypasslist>
          </defaultProxy>
          ```

    - Note that the value of “address” is a regular expression.

- Save and close the file

- Restart the service NEC Remoting Service or the Business ConneCT computer

Social Media Proxy service

The NEC Social Media Proxy service communicates with Social Media Providers. By default a connection to a Social Media Provider will not go through a proxy server. If the Social Media Providers can only be accessed from the BCT computer through an internet proxy then you must configure the proxy settings.

On the Business ConneCT server:

- Browse to "C:\Program Files (x86)\Common Files\NEC\ Social Media Proxy " and use a text editor (e.g. Notepad) to open the file “appsettings.json”. Make sure the file contains a section “NetworkProxy” and in this section add a key-value pair “Address”: “<proxyURI>”. For example:

```
{
  "NetworkProxy”: {
    "Address": "http://192.168.100.60:8080"
  },
  "Logging": …
```

- Save and close the file
- Restart the service NEC Social Media Proxy or the Business ConneCT computer

See 11.3.17 Social Media Proxy service logging about logging of the Social Media Proxy service.

33. Appendix W – Web Chat UIP Integration

Besides routing chat messages (both webchat and social media) to agents it's possible to route chat messages to UIP (Univerge Integration Platform). This integration can be used for instance to route chat messages to a chat bot system.
This feature can be enabled, when BCT – UIP integration is available, by creating user(s) with a Virtual Agent role. These Virtual Agents must be member of a group which is assigned to a router handling the chat messages. When virtual agents are present in the system for such a router, BCT will attempt to route the chat requests to UIP and UIP may accept or reject this chat-request within 10 seconds. When the request is not accepted in time or it is rejected, the chat request will be offered to a regular BCT agent, resulting in the usual BCT behavior.

UIP must use the dedicated BCT adapter commands to accept or reject chat requests and to react to chat messages. The exact name of the virtual agent user must be used by UIP in order to accept or reject a chat request.

In case a chat is accepted by a real agent, BCT will automatically send the text of prompt 620 ("Thank you for waiting. My name is {…}. How can I help you") to the customer. In case a chat is accepted by a virtual agent, BCT will not send the text of this prompt. In this case, the workflow of UIP is responsible to send a similar message and 'continue' the conversation.

UIP can also be used to create a chat menu that allows the chat (webchat and social media) to be handled on a different router, depending on the chosen menu option. An example of such a menu is available in a separate document.

34. Appendix X – Security Advisor

Security affects everyone and a lack of security is a real risk for organizations; a security breach can potentially disrupt all normal business and bring your organization to a halt. Therefore this appendix will advise you on some security aspects with respect to the Business ConneCT server and its hosted web applications.

For the Business ConneCT server IIS hosted web applications next potential vulnerabilities are addressed (i.e. security risks are mitigated or fixed):

Security Vulnerability	Additional Info
Cross-site Scripting	• HTTP OPTIONS web requests are disabled for IIS "Default Web Site" • HTTP responses will contain security headers 'Content-Security-Policy', 'X-Content-Type-Options' and 'X-XSS-Protection'
Click Jacking	• HTTP responses will contain security header 'Content-Security-Policy' and for IE11 compatibility also the 'X-Frame-Options' header
Revealed Platform Info	• HTTP responses will not contain headers 'Server', 'X-AspNet-Version' and 'X-Powered-By'

Besides the above mentioned aspects that are addressed by Business ConneCT itself (taken care of by configuring IIS during the installation) next listed possible vulnerabilities might apply for your system.

When this is the case the related recommendations (remediation steps) should be seriously considered for your Business ConneCT server.

Note: the order of the list below is arbitrary and does not indicate any priority

Security Vulnerability	Remediation Steps
Microsoft IIS default installation/welcome page installed	• The default page should be replaced with relevant content.
Untrusted TLS/SSL server X.509 certificate or self-signed TLS/SSL certificate	• Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.
TLS/SSL Server supports unsecure vulnerable TLS/SSL protocol versions. For example: the SSL v3 protocol and supported ciphers all suffer from serious vulnerabilities making this protocol unsafe to use.	• Minimum step is to disable unsecure SSL v3 and TLS v1.0 protocols • It is recommended to migrate to a minimum of TLS v1.1 preferably TLS v1.2 as for example indicated by Payment Card Industry (PCI) Data Security Standard and FIPS 140-2 standard.
TLS/SSL Server supports unsecure non-strong (weak) Cipher suites. For example: Server supports 3DES Cipher Suite, RC4 Cipher Algorithms or might use Static Key Ciphers	• Configure your server to only support strong ciphers (or cipher suites) • So disable support for 3DES suite, RC4 ciphers and static key ciphers. • Please view the article in the Microsoft Knowledge Base 245030 "How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll"

Security Vulnerability	Remediation Steps
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	• Configure your server to disable support for 3DES ciphers • Please view the article in the Microsoft Knowledge Base 245030 “How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll”
Click Jacking on SafeNet 'Sentinel Protection Server'	• In case you are not using an HW (USB) dongle but for example LMC for licensing please uninstall “Sentinel Protection Installer 7.6.9” • In case you are using an HW (USB) dongle for licensing best approach is to uninstall feature ‘Sentinel Protection Server’ via ‘Change’ of ‘Sentinel Protection Installer 7.6.9’ package from ‘Programs and Features’
ICMP timestamp response	• Disable ICMP timestamp responses on your Windows system • The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).
TCP timestamp response	• Disable TCP timestamp responses on your Windows system • If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets
Weak LAN Manager hashing permitted	• Make sure to update your network authentication settings to allow the use of NT LAN Manager version 2 (NTLMv2) only. • Please see Microsoft article “Security guidance for NTLMv1 and LM network authentication” for details.

Additional references that may assist you in handling the security aspects for the server:

- Windows Server 2016 Security Guide.
  This paper includes general guidance for helping secure servers in your environment as well as specific pointers on how you can utilize new security features in a Windows Server 2016.
- Windows Security Baselines / Microsoft Security Compliance Toolkit
  This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.