Mitel MiVoice Connect Contact Center Installation Guide

May, 2024

Trademarks

Version Information

Mitel MiVoice Connect Contact Center Installation Guide
Date: March 15, 2024

Company Information

Mitel Networks Corporation
350 Legget Dr.
Kanata, Ontario K2K 2W7
Canada
+1.844.937.6483

Table of Contents

Before You Start

About This Book

ShoreTel is now part of Mitel. Together, we look forward to helping you power connections that are brilliantly simple.

The Connect Contact Center Installation Guide describes how to get your Connect Contact Center system up and running. In this guide, you will find:

- Introduction to Connect Contact Center
- Hardware and software requirements
- Installation instructions
- Directions for setting up Connect Contact Center
- Information about testing the Connect Contact Center system
- Overview of upgrading, maintaining, and troubleshooting Connect Contact Center

This guide is intended for professional services engineers or technical personnel responsible for system installation. This guide also provides getting started information for Connect Contact Center administrators and other system users, as well as a basic overview of the applications that make up the Connect Contact Center system.

Organization

The document is divided into the following chapters:

- Chapter 1, Introduction
- Chapter 2, Hardware and Software Requirements
- Chapter 3, Installing Connect Contact Center
- Chapter 4, Setting Up Connect Contact Center
- Chapter 6, Upgrading, Maintaining, and Troubleshooting Connect Contact Center

Conventions

The following typographical marking conventions are used in this document.

Marking	Meaning
Bold	Names of interface objects, such as buttons and menus.
`Courier`	Code examples.
`Courier Italic`	Variables in code examples.
Blue	Cross references with hyperlinks. Click the blue text to go to the indicated section. All chapters have a list of section links on the first page. **Note:** Table of Contents entries are also links, but they are not shown in blue.

CHAPTER

1

Introduction

Connect Contact Center is an enterprise-class call center solution that offers advanced, multimedia call routing, a sophisticated built-in Interactive Voice Response (IVR) system, advanced reporting, and powerful integration into business applications through open interfaces.

Refer to the following sections for more information about Connect Contact Center:

Connect Contact Center Components

A basic Connect Contact Center Solution includes the following components:

Connect Contact Center Module	MiVoice Connect	MiCloud Connect
Connect Contact Center Director	X	X
Diagnostics Console	X	
Connect Contact Center Historical Reports	X	
Agent Manager	X	X
Interaction Center	X	X
Graphical Call Control Script (GCCS) Administration	X	X

Connect Contact Center Server

The Connect Contact Center Server software provides an intelligent routing engine and an integrated interactive voice response (IVR) package for managing call center configuration, call activity, and reporting, and for implementing the required routing plan. The server software runs on a dedicated server at your call center.

The Connect Contact Center Server may be at the same location as the ShoreWare Headquarters Server. The Connect Contact Center Server is a ShoreWare distributed server with the Connect Contact Center Server software also installed. In a production environment, the Connect Contact Center applications should **not** be run from the Connect Contact Center Server.

The Connect Contact Center Server and standalone IVR servers can also be deployed as virtual machines on the VMWare platform.

The Connect Contact Center Server interacts with the Mitel Connect system as a TAPI application.

Supervisor Components

The Supervisor application is used to administer and monitor call center activities, and to report on real-time and historical information that details or summarizes the system's performance over a specified time period. Supervisors cannot start or stop the Connect Contact Center system.

The Connect Contact Center supervisor applications are:

- Connect Contact Center Director is used to configure the Connect Contact Center entities and set system parameters.
- Graphical Contact Center Scripting (GCCS) Administration is a tool used to design business logic with functions used in any kind of call flow, such as inbound, outbound, email, and chat calls.
- Agent Manager furnishes real-time statistical information on call center activities. The information can be displayed in tables, forms, and graphical formats.
- Interaction Center provides agents and supervisors with access to telephony and ACD capabilities as well as to key performance indicators (KPIs). Supervisors can silently or interactively monitor agent interactions using Interaction Center.

  The Interaction Center is available at the following URL:

  - If the HTTPS for Connect Center Clients is enabled during installation, use https://<*contact center server IP address or FDQN*>:8433/ccd.
  - Otherwise, use http://<*contact center server IP address*>:3000/ccd.

Note

For information about handling insecure connection error messages on the browser, see the section *Browser warning message* in the *MiVoice Connect Contact Center Administration Guide*.

Tip

The wecc.ini file may need to be manually changed if a FDQN is used for the HTTPS certificate. Refer to Troubleshooting Authentication and Bootstrapping on page 35.

- Connect Contact Center Historical Reports allows supervisors to generate predefined and custom reports on historical call center activity. With this information, management can efficiently allocate personnel to meet staffing requirements.
- Connect Contact Center Diagnostics Console is used to diagnose and remedy basic system problems.

New Installations

The software license keys must be installed before you can use Connect Contact Center, as explained in Installing the Connect Contact Center Software License Keys on page 31.

Connect Contact Center uses a system key. The system key you initially receive is not node-locked. You use this non node-locked system key to install and initially use Connect Contact Center. You then have 45 days to request and enter the required node-locked system key, while continuing to use Connect Contact Center. During this grace period, when you log into Connect Contact Center Director or any other supervisor application, a message is shown specifying the number of days remaining.

If you do not enter a node-locked system key during this period, the system enters lockdown mode. In lockdown mode Connect Contact Center Director only displays the License pages, which you can use to enter a node-locked system key. You are unable to log into any other Connect Contact Center supervisor application or run scheduled reports. However, call routing and agent activities are maintained.

Note: If you are using Windows Server 2008 R2 as your Connect Contact Center server operating system, Windows Server 2008 R2 must be installed before requesting a node-locked system license key. If you are upgrading Server 2008 R2, first enter the Connect Contact Center node-locked system key.

You request and enter the node-locked system key using Connect Contact Center Director. For information, refer to Requesting and Entering a Node-Locked System Key on page 39.

Upgrades

Access to the features that you have previously purchased are maintained when you upgrade from MCCC 9 to Connect Contact Center with the following exceptions:

- Agent Toolbar has been deprecated. Interaction Center replaces this functionality.
- Wallboard has been deprecated. Interaction Center replaces this functionality.
- Communicator has been deprecated. Connect client replaces this functionality and currently does not integrate with Interaction Center.

Viewing License Information

To view license information in Connect Contact Center Director, click **Maintenance** > **License** > **License Keys** > **Current Licenses**. Information about the current licenses appears, including the license key, license type, and number of licenses of that type that you have.

The following list includes possible license types:

- **System** — The node-locked system license key required for all systems.
- **Voice** — The maximum number of agents, who log into a group that requires a license to handle incoming and outbound voice calls, that can be logged into the system concurrently.
- **Email** — The maximum number of agents, who log into a group that requires a license to handle incoming email contacts, that can be logged on the system concurrently.
- **Chat** — The maximum number of agents, who log into a group that requires a license to handle incoming chat contacts, that can be logged into the system concurrently.
- **Dial Lists** — The maximum number of agents, who log into a group that requires a license to handle outbound dial lists calls, that can be logged into the system concurrently.
- **IVR Ports** — The maximum number of IVR ports the system will use. Note that you can define additional IVR ports beyond the number for which you are licensed. This allows you to use IVR stations to create redundant IVR stations.
- **Supervisor** — The maximum number of supervisors that can be logged into the system concurrently.

  Connect Contact Center currently supports up to 100 concurrent supervisors.
- **Redundancy** — Enables running the Connect Contact Center system in a redundant configuration.
- **Agent Activity API** — The number of external applications able to connect and receive agent data.
- **Group Activity API** — The number of external applications able to connect and receive group data.

Connect Contact Center System Maximum Scale

This section contains a table that shows the maximum values for parameters in the current release of Connect Contact Center. See Hardware and Software Requirements, starting on page 9 for the hardware and software requirements for supporting different scopes of a Connect Contact Center deployment, from the smallest to the largest supportable Connect Contact Center.

Contact Center MiVoice Connect Element	Maximum number or value
Max Configured Agents	2000
Max Simultaneous Agents	500 or 1000*
Max DNIS Routes	1500
Max Number of Voice and Chat Groups	1000
Number of Agent Queues	1000
Number of Email Agent Queues	1000
Max number of groups to which an agent can belong	64
Max Skills	512
Max Release Codes	1000
Max Wrap Up Codes	1000
Max Secondary Announcements	20
Max IVR Ports per system	1000
Max Calls in Queue per server	254
Max Configured Supervisors	400
Max Active Supervisors	200
Database Backup Periodicity	1 a day
Maximum interactions	12,500
Max IRN	1500
Maximum number of scheduled reports in an hour	100 per 15 minute interval
Maximum Event Feed API Connections	400
Maximum number of scripts (100 actions per script)	500
Maximum number of schedules	TBD
Max Number of Agent COS	1000
Max Number of Voice and Chat Services	1000
Max Number of Email IRNs	1500
Max Number of Email Services	1000
Max Number of Email Groups	1000
CCIR Enabled?	Yes

*To support 500 simultaneous agents, the system must have 8 cores and 8 GB of RAM. To support 1000 simultaneous agents, the system must have 16 cores and 16 GB of RAM.

CHAPTER

2

Hardware and Software Requirements

This chapter provides information on the Connect Contact Center hardware and software requirements in the following sections:

Connect Contact Center Server Requirements

Connect Contact Center server software must run on a dedicated computer that meets or exceeds the hardware and software requirements as described in this chapter, and is attached to the network. This chapter defines three levels of requirements, based on the type of call center, normal loads, and activity.

For high call loads and advanced interactive voice response (IVR) activity, including large numbers of Dialed Number Identification Services (DNIS), more than 150 concurrent agents, and more than 1,000 calls per hour, please contact Mitel Customer Service. The support of more than 150 simultaneous users, or more than 1,500 simultaneous media ports, requires multiple servers to separate the core Connect Contact Center and IVR engines.

Connect Contact Center runs as a Microsoft Windows service with multiple child processes and conforms to standard service semantics, such as Start, Stop, and Restart.

Depending on how your call center is set up, and the location of your agents, the server allocation recommended in this chapter should be followed to reduce latency.

The Connect Contact Center Server and standalone IVR servers and dedicated standalone servers for CCIR data can also be deployed as virtual machines on the VMWare platform. For information, see System Requirements for a Virtualized Deployment on page 14.

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

Server Allocation

Typically, the HQ (PBX HQ) and Connect Contact Center servers should reside at the same physical location. However, if your call center includes agents in a remote location that uses a Distributed Voice Server, the Connect Contact Center server should be at the remote location to reduce network latency and improve agent experience with Connect Contact Center.

It is highly recommended that the site that has the Connect Contact Center server always have either an HQ server or a DVS server with which the agents at the site are associated.

System Requirements

The components required to support Connect Contact Center Server software vary based on the number of simultaneous agents you plan to support in your call center.

System Requirements for Less Than 300 Simultaneous Agents

The following components are required to support Connect Contact Center Server software for less than 300 simultaneous agents:

- One Processor Server to run the main Connect Contact Center core engine, and if more than 250 IVR ports are used, one additional server to run the standalone distributed IVR ports.

  The servers can be one of the following

- Intel Core 2 Duo E8400 Single DualCore
- Intel Core i3-540 Processor
- Intel Xeon 3430 Single QuadCore

  Refer to Processors and Memory on page 21 for information about the server processor requirements.

- Memory

  Refer to Processors and Memory on page 21 for information about the server processor requirements.

- Hard drive free disk space requirement - 200 GB
- DVD
- Keyboard
- A standard Windows keyboard.
- Monitor and Mouse
- First Network Adapter (TCP/IP)
- Second Network Adapter (TCP/IP) (Optional)
- Operating System

  Refer to Operating Systems for Stations on page 16 for details.

- Core Platforms

  Refer to Supported Unified Communication Platforms on page 17 for information.

System Requirements for 300 to 599 Simultaneous Agents

The following components are required to support the Connect Contact Center Server software for up to 599 simultaneous agents.

- One Processor Server to run the main Connect Contact Center core engine, and depending on the number of IVR ports used, an additional one to three servers to run the standalone distributed IVR ports. The servers to run the IVR ports can be one of the following:
  - Intel Core 2 Duo E8400 Single DualCore
  - Intel Core i3-540 Processor
  - Intel Xeon 3430 Single QuadCore
  - Hard drive free disk space requirement - 200 GB

  Refer to Processors and Memory on page 21 for information about the server processor requirements.

- One Intel Xeon 5520 Single QuadCore server to run the main Connect Contact Center core engine.
  - Hard drive free disk space requirement - 500 GB
- Memory

  Refer to Processors and Memory on page 21 for an explanation of the memory requirements.
- Backplane
- 1X6 Hot-Pluggable HDD Backplane
- DVD
- Keyboard

  A standard Windows keyboard.
- Monitor
- Mouse
- First Network Adapter (TCP/IP)
- Second Network Adapter (TCP/IP)
- Serial Port #1
- Serial Port #2 (Optional)
- Power Supply Kit

  Redundant Power Supply 2+1
- Operating System

  Refer to Operating Systems for Stations on page 16 for details.
- Core Platforms

  Refer to Supported Unified Communication Platforms on page 17 for information.

System Requirements for 600 to 1,000 Simultaneous Agents

The following components are required to support the Connect Contact Center Server software for up to 1,000 simultaneous agents.

- One Processor Server to run the main Connect Contact Center core engine, and depending on the number of IVR ports used, up to four additional servers to run the standalone distributed IVR ports.The servers to run the IVR ports can be one of the following:
  - Intel Core 2 Duo E8400 Single DualCore
  - Intel Core i3-540 Processor

- Intel Xeon 3430 Single QuadCore
- Hard drive free disk space requirement - 200 GB

Refer to Processors and Memory on page 21 for information about the server processor requirements.

- One Intel Xeon 5520 Dual QuadCore server to run the main Connect Contact Center core engine.
  - Hard drive free disk space requirement - 750 GB
- Additional Processor (if required)
- Memory

  Refer to Processors and Memory on page 21 for an explanation of the memory requirements.
- Backplane

  1X6 Hot-Pluggable HDD Backplane
- DVD
- Keyboard

  A standard Windows keyboard.
- Monitor
- Mouse
- First Network Adapter (TCP/IP)
- Second Network Adapter (TCP/IP)
- Serial Port #1
- Serial Port #2 (Optional)
- Power Supply Kit

  Redundant Power Supply 2+1
- Operating System

  Refer to Operating Systems for Stations on page 16 for details.
- Core Platforms

  See Supported Unified Communication Platforms on page 17 for information.

System Requirements for a Virtualized Deployment

Connect Contact Center can be deployed as an application on a virtual machine on the VMWare platform. This allows Connect Contact Center to be part of a virtualized deployment, resulting in savings due to server consolidation and reduced total cost of ownership.

For standalone IVR servers and standalone servers used for CCIR data, use the sizing for a small system. The recommended virtualized sizing appears in the following table.

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

System Size	# of Agents	Call Load Per System	Cores Per VM	RAM per VM	Free Disk Space for Connect Contact Center Server
Small	< 100	7,500	2	4 GB	200 GB
Medium	100-599	15,000	4	8 GB	500 GB
Large	600-1,000	10,000	4	8 GB	750 GB

For information about DVS server support and installation, refer to the *Mitel Connect Planning and Installation Guide*.

System Requirements for a Virtual Deployment of Edge Gateway

The Edge Gateway is a remote access solution offering for Mitel customers who are using a MiVoice Connect solution. The Edge Gateway makes it possible for users to connect remotely to the Mitel network by using a Mitel appliance, such as an IP phone or the Mitel Connect Unified Communications Client. Refer to the *Mitel Connect Edge Gateway Administration Guide* for information about the system requirements for this feature.

Note

Mitel MiVoice Connect Contact Center supports only one primary contact center server and one redundant contact center server per headquarters system.

CCIR System Requirements

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

The amount of time it takes to upgrade a large CCIR database is dependent on the performance of the server. Consider the database size and the processor performance of your hardware configuration when planning a CCIR upgrade or conversion.

System Requirements for a CCIR Deployment

For CCIR systems, the recommended hardware, which is newer model Xeon processor and 10,000 rpm HD, or virtualized sizing appears in the following table:

System Size	Million Number of Records	Call Load Per System	Cores Per VM	RAM per VM	Disk Size (10k RPM disk)
Small	< 100	7,500	2	4 GB	Refer to Disk Size Calculation
Medium	100-200	15,000	4	8 GB	Refer to Disk Size Calculation
Large	> 200	10,000	4	8 GB	Refer to Disk Size Calculation

Disk Size Calculation

Retention Time (days) x Avg. Number of Calls per day x 60 records per call. For example, 730 (2 years) x 60,000 x 60 = 2,628,000,000 records. On average, one record is approximately 350 bytes, which equals 919,800,000,000 bytes or approximately 860GB.

In addition to the required disk space for the data, consider upgrade space, which is twice the database size. If the same disk is used for CCIR backups, also consider backup space.

CCIR System Requirements for Large Databases

The amount of time it takes to upgrade a large CCIR database is dependent on the performance of the server. Consider the database size and the processor performance of your hardware configuration when planning a CCIR upgrade or conversion.

Note

The hard drive disk capacity of the server must be greater than twice the database size.

For example, an internal Mitel upgrade of a CCIR database with more than 235 million records required a virtual machine with the following configuration.

- 2 CPUs
- 4GB RAM
- Intel® Xeon® Processor E5630
- 10,000 rpm SCSI HD

For information about DVS server support and installation, refer to the *Mitel Connect Planning and Installation Guide*.

Operating Systems for Stations

Connect Contact Center requires the following operating systems:

- Server station
  - Microsoft Windows Server 2008R2 64-bit, Standard, and Enterprise
  - Microsoft Windows Server 2012R2/Hyper-V, Standard, and Datacenter
  - Microsoft Windows Server 2016, Standard, and Datacenter
  - Microsoft Windows Server 2019, Standard, and Datacenter
- IVR Distributed Server station
  - Microsoft Windows Server 2008R2 64-bit, Standard, and Enterprise

- Microsoft Windows Server 2012R2/Hyper-V, Standard, and Datacenter
- Microsoft Windows Server 2016, Standard, and Datacenter
- Microsoft Windows Server 2019, Standard, and Datacenter

- Supervisor station
  - Microsoft Windows 7 Professional and Enterprise (32-bit and 64-bit) versions
  - Microsoft Windows 8 Pro and Enterprise (32-bit and 64-bit) versions
  - Microsoft Windows 8.1 Pro and Enterprise (32-bit and 64-bit) versions
  - Microsoft Windows 10

Supported Unified Communication Platforms

The following releases of Unified Communication software support Connect Contact Center:

- Mitel Connect

Supported Browsers

The following browsers are supported for running Connect Contact Center Director, supervisor applications, and Mitel Interaction Center:

- Microsoft Internet Explorer (IE) 10 and 11
- Microsoft Edge
- Firefox, on Windows and Apple OS X
- Chrome, on Windows and Apple OS X
- Safari, on Apple OS X

Supported Virtual Machines

The following are supported:

- VMWare 6.0 ESX/ESXi
- VMWare 6.5 ESX/ESXi
- VMWare 6.7 ESX/ESXi

- Microsoft Windows Server 2012 R2 (VMWare / Hyper-V)
- Microsoft Windows Server 2016 (VMWare / Hyper-V)
- Microsoft Windows Server 2019 (VMWare / Hyper-V)

VMWare Tools

Connect Contact Center supports the following VMWare configuration tools:

- High Availability
- VMWare vMotion

Bandwidth Usage

This section describes the bandwidth usage for the Connect Contact Center applications Agent Manager.

Bandwidth Usage for Agent Manager

Bandwidth consumed between the Connect Contact Center Server and Agent Manager varies depending on the number and type of open real-time reports, such as the number of groups and number of agents, and the Agent Manager update timer interval.

Information is sent once at every update timer interval. Agent information is passed for each agent in a group report. Group information is passed for each group an agent is logged into. Also, the Agent Manager Login Manager and opened minimized reports add small incremental bandwidth consumption when used.

Because of the wide variety of display options in Connect Contact Center real-time reports, a fixed bandwidth consumption estimate cannot be provided. However, the following benchmarks provide an idea of the consumed bandwidth. The bandwidth estimate at the end of each of the following examples reflects the Connect Contact Center configuration and hypothetical loads.

Example 1

Configuration

- Call load: 2,800 calls per hour
- Call duration (per call): 10 seconds
- Agents: 8 agents logged in
- Groups: Each agent logged in to 2 groups

Open Reports

- 2 Group reports
- 2 Agent reports

Agent Bandwidth Usage by a Manager

- Average: 30 KBytes/sec

Example 2

Configuration

- Call load: 300 calls per hour
- Call duration (per call): 10 seconds
- Agents: 1 agent logged in
- Groups: Each agent logged in to 2 groups

Open Reports

- 2 Group reports open
- 1 Agent report open
- 1 STI report open

Agent Bandwidth Usage by a Manager

- Average: 12 KBytes/sec

Example 3

Configuration

- Call load: 530 calls per hour
- Call duration (per call): variable
- Agents: 80 agents logged in (average)
- Groups: Each agent logged in to 4 groups (average)

Open Reports

- 2 Group Agent Status reports open with ~ 40 agents in each group
- 4 Group Agent Status reports open with ~ 7 agents in each group
- 1 Brief Group Status report open containing 11 groups

Agent Manager Bandwidth Usage

- Average: 8.5 KBytes/sec

Reserved Ports

Table 1 shows the ports that must reserved for Connect Contact Center use.

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

Table 1: Reserved Ports

Contact Center Element	HTTP/TCP Port	HTTPS/TLS Port	External Port
Contact Center Director	31459	31461	—
Interaction Center	3000	8433	—
CAC	31452	—	—
Contact Center Event Feed API	31458	—	—
Redundant Interaction Center	8080	—	—
External CCIR System	6306	—	—

Processors and Memory

The following table summarizes the server processor and memory requirements:

Server	Minimum CPU	Minimum RAM	Network	Free Disk Space
Intel Core 2 Due E8400 Single Dual Core	3.00 GHz	4 GB	100 Base-T or Gigabit Ethernet	200 GB
Intel Core i3-540 Processor (4M Cache)	3.06 GHz	4 GB	100 Base-T or Gigabit Ethernet	200 GB
Intel Xeon x3430 Single Quad Core	2.4 GHz	4 GB	100 Base-Tor Gigabit Ethernet	200 GB
Intel Xeon e5520 Single Quad Core	2.27 GHz	8 GB	100 Base-T or Gigabit Ethernet	500 GB
Intel Xeon e5520 Dual Quad Core	2.27 GHz	8 GB	100 Base-T or Gigabit Ethernet	750 GB

For dual CPU configurations, use the following formula to estimate the total frequency of the system: (CPU#1_frequency + CPU#2_frequency) *0.8.

Remote Access

The Connect Contact Center Server should be configured for remote access maintenance and support operations. You must enable Terminal Services on the server to allow administrators to connect using Terminal Services Client software.

Connect Contact Center Clients

Connect Contact Center supervisor client applications run on the user's PC alongside any other applications.

The following tables summarize the minimum requirements for the Supervisor PC running Connect Contact Center.

Hardware Components	Specification
Agent or Supervisor PC Running Connect Contact Center only	Windows 7 Windows 8 Windows 8.1 Windows 10 Enterprise and Professional 32-bit and 64-bit Operating System
CPU	Dual-Core
RAM	4 GB
Hard Disk	60 GB
CD	Optional
First Network Adapter	10/100 Mb
External Modem	Optional

CHAPTER

3

Installing Connect Contact Center

This chapter describes how to install Connect Contact Center. It includes details for installing and uninstalling Connect Contact Center in a thin client environment.

Refer to the following sections for more information:

The Connect Contact Center Server software and Connect Contact Center applications support redundancy from the server. We recommend redundancy to minimize system down-time and improve the recovery process if the hardware fails. Refer to the *Mitel Connect Contact Center Administration Guide* for information on installing and using the Mitel redundant server system.

Installation Prerequisites

Before beginning the Connect Contact Center installation, verify that the following prerequisites have been met:

- A dedicated server is available for installing the Connect Contact Center Server.
- The Connect Contact Center Server has assigned static IP addresses.
- You are familiar with the supported Microsoft Windows server environments.
- You have local administrator privileges to install and execute Connect Contact Center applications on the Connect Contact Center Server.
- Beginning with Release 19.3, you must use Adopt Open JRE 1.8.0.212 or a later version.

Note

During the upgrade, JRE 1.6 version will be uninstalled. If it is not uninstalled, you must manually uninstall it.

- If the **HTTPS for Contact Center Clients** is enabled during installation, it is strongly recommended to use a certificate issued by third party trusted certificate authority. A certificate for use with HTTPS is required and must be issued to a fully qualified domain name, which means that a name server such as DNS is required for this configuration.

All server and client computers must connect over a LAN that supports TCP/IP. Mitel recommends that you assign static IP addresses for the Connect Contact Center Server. Supervisor workstations can use Dynamic Host Configuration Protocol (DHCP) if it is available.

Required Installation Information

Prior to installing the system components, make sure that you have the following required information:

- The Connect Contact Center Server static IP addresses.
- The Connect PBX server IP addresses.
- Your power source.
- Specifics on agent telephone extensions.

Static Server IP Addresses

The Connect Contact Center Server should have static IP addresses. Mitel considers the assignment of static IP addresses for servers to be a best practice.

Power Source

Ensure that the Connect Contact Center Server has a protected power source, such as an uninterruptable power supply (UPS).

Installing the Distributed Server Software

Before installing the Connect Contact Center Server software, you must install and configure the ShoreGear Softswitch Distributed Voice Server (DVS) that you will use to host the Connect Contact Center system. Refer to the Distributed Voice Server Software Installation section of the *Mitel Connect Planning and Installation Guide* for information about this installation procedure.

Note

Connect Contact Center can be installed only on a Windows DVS.

Before adding the distributed server, note the following:

- On systems containing two network interface cards (NICs), disable one card.
- Do not change the pre-set voice mail extensions.
- Do not enable or configure the Simplified Message Desk Interface (SMDI).
- In Connect Director on HQ, navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**, select the ShoreGear Softswitch appliance you have Connect Contact Center installed on, and make sure that **Allow Voice Mailboxes** is *not* selected in the **Voice Application** tab.

Installing the Connect Contact Center Server

Once you have installed the ShoreWare Distributed Server software, you install the Connect Contact Center Server on the same server.

Note

To convert Connect Contact Center from http to https operation, you must start the Contact Center installer and select the **Enable HTTPS for Contact Center Clients** check box.

Tip

These steps also apply when you are installing a secondary contact center server in a redundant configuration.

Prerequisites

- Verify that the server meets the basic requirements, as specified in Chapter 2 Hardware and Software Requirements.
- Verify that the server is connected to the network and has a static IP address.
- If the computer has two enabled NICs, disable the NIC not running the *Mitel Remote Telephony Application Programming Interface (TAPI) Service Provider*.

  If a server has two enabled NICs, you might not be able to install or upgrade the Connect Contact Center server software correctly.
- Turn on the server.

A common browser error that appears in Google Chrome when one attempts to view web sites hosted on IIS7 on Windows Server 2016 and Windows Server 2019, caused by HTTPS handshake failure is: **ERR_SPDY_INADEQUATE_TRANSPORT_SECURITY.** If you are installing Connect Contact Center on Windows Server 2016 or Windows Server 2019 and enabling HTTPS, you can resolve this error during installation.To resolve the error, use one of the following methods:

- Change the available HTTPS ciphers using the registry keys available for the ciphers. For details about the cipher registry keys, see https://support.microsoft.com/en-us/help/245030/how-torestrict-the-use-of-certain-cryptographic-algorithms-and-protoc.

  Alternatively, you can modify the ciphers without editing the Windows registry using the IIS Crypto 2.0 program. For details about the IIS Crypto 2.0 program, see https://www.nartac.com/Products/IISCrypto.Disabling HTTP/2 on IIS of the Windows server 2016.
- Do either of the following depending on the server version:
  - **For Windows Server 2016:** Disable HTTP/2 on IIS of the Windows Server 2016.
  - **For Windows Server 2019:** Disable HTTP/2 on IIS of the Windows Server 2019.

Install Procedure

Complete the following steps to install the Connect Contact Center Server software:

1. Log in to the server as a Windows Administrator.
2. Navigate to the Mitel support site, download the Connect Contact Center installer, and then run the `setup.exe` file.
3. Click **Install** when the installer prompts you for the redis and nodejs objects.
4. Click **Next** to continue.

   If you decide to stop the installation, click **Cancel** at any time throughout the process. If you want to return to the previous screen, click **Back**.
5. Click **Next** when the installer prompts you to accept the terms of the license agreement.
6. The following information is automatically populated based on information you specified earlier in the installation process:

   - **Fully Qualified Domain Name of Server**: This is the Connect Contact Center server. If you are not using a naming service, such as WINS, on your server, enter the IP address of the DVS.

Tip

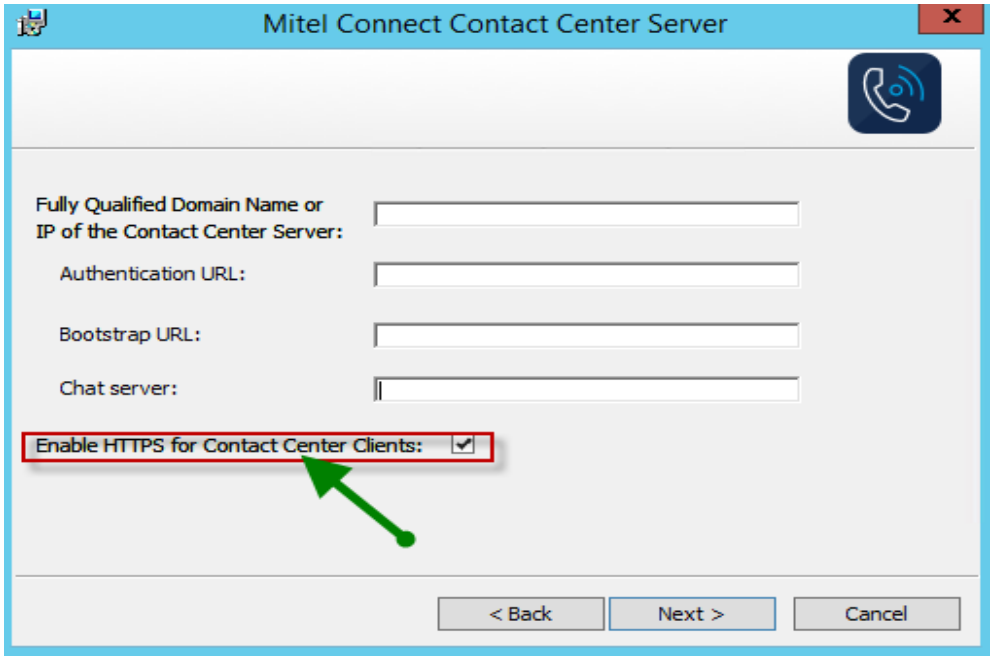
If you are installing on a secondary contact center server, the Fully Qualified Domain Name of Server is the FQDN or IP address of the secondary server.

Note

To launch the Connect Contact Center Director, it is recommended that you use an FQDN instead of the IP address if the HTTPS and client security is enabled. Otherwise, the web browsers will encounter certificate issues and display the warning messages.

   - **Authentication URL**: https://<*Connect headquarters server IP address*>/shoreauth
   - **Bootstrap URL**: https://<*Connect headquarters server IP address*>/shorestart
   - **Chat URL**: If you use chat, this is the Tomcat server IP address. Otherwise, this is the IP address of the Connect Contact Center server.

- To enable HTTPS support, select the **Enable HTTPS for Contact Center Clients** check box.



7. In the Destination Folder screen, click **Next** to keep the default destination and continue the installation.

   The default destination is `C:\Program Files (x86)\ShoreTel\Contact Center Server`.

   Alternatively, you can click **Change** to locate and select a different destination folder, and then click **Next**.

8. In the resulting screen, click **Install** to begin installation of the server software.

   During the installation process, all files are installed into the appropriate directories. While the files are being installed, a status bar shows the progress of the process.

   a. Copy the following three certificate files from the HQ server to the `<installation location>\ShoreTel\ShoreTel Contact Center Server\Bin` directory on the Connect Contact Center Server server:

      - c:\Shoreline Data\keystore\certs\BootstrapData.crt
      - c:\Shoreline Data\keystore\certs\hq_ca.crt
      - c:\Shoreline Data\keystore\private\BootstrapData.key

      If these three files are not on the HQ server, complete the following steps to generate them. Otherwise, proceed to step 9.

      a. On the HQ server, open a command prompt.

      b. Change directories to the Connect installation location, and then run bin\pki.bat -S BootstrapData as shown in the command sample below.

```
cd "<installation location>\Shoreware Director\App"
bin\pki.bat -S BootstrapData
```

9. If you do not want to use the Connect Contact Center Server immediately, deselect **Start ShoreTel Connect Contact Center Server Now**, and then click **Finish** to complete the server installation process.

   Restart the contact center service. Optionally, you can restart the server to ensure that all contact center and related services are restarted.

Post-Installation Configuration

Configure virus scan folder exclusions as follows:

- Supervisor Systems:

  ```
  <Drive>:\Users\%User%\AppData\Roaming\ShoreTel Contact Center
  <Drive>:\Users\%User%\AppData\Local\ShoreTel Contact Center
  ```

- DVS Server:

  ```
  <Drive>:\Program Files (x86)\Shoreline Communications
  <Drive>:\Shoreline Data\
  ```

Certificates

The Connect Contact Center system uses self-signed certificates. If you prefer to use a third-party certificate, follow the procedure in the Importing a Certificate for HQ and DVSs section of the *Mitel Connect System Administration Guide* to import certificates to your Headquarters (HQ) server. The DVS that hosts Connect Contact Center will retrieve those certificates for use on the contact center.

Note

When following the procedure to import third-party certificates to the HQ, ensure that the root certificate is copied and stored in the same location as the intermediate certificate in addition to being loaded on the HQ.

Troubleshooting Authentication and Bootstrapping - IP Addresses

During installation, the administrator configures authentication and bootstrapping, identifying the contact center server, the authentication server, the bootstrapping server, and the tomcat server if chat is enabled. If there are any issues with this configuration, such as mistakenly entering the incorrect IP address for Connect HQ or the contact center server, complete the following steps:

1. Open each of the following files in a text editor, such as Notepad.exe, and modify HQ and contact center server IP addresses as necessary:

Table 1: Contact Center Configuration File Contents

Configuration File	IP Addresses
wecc.ini	■ Contact Center FQDN ■ <FQDN or IP address of the authentication server>/shoreauth ■ <FQDN or IP address of the authentication server>/shorestart
WebAgentFramework.ini	■ Contact Center FQDN ■ <FQDN or IP address of the authentication server>/shoreauth ■ <FQDN or IP address of the authentication server>/shorestart ■ Tomcat server IP address, which is applicable only if you use chat.
EventFeedAPIFramework.ini	Note: This file is applicable only if you have developed applications using the Event Feed API. ■ Contact Center FQDN ■ <FQDN or IP address of the authentication server>/shoreauth ■ <FQDN or IP address of the authentication server>/shorestart
registry.ini	■ FQDN or IP address of the contact center server

2. Restart the Connect Contact Center service.

Installation Tree Structure

For reference in the event of a rollback, the following list details the installation structure and contents.

- Backup — This directory contains backups of contact center databases unless the system administrator has chosen a different location in which to store backups.
- Bin — This directory contains all binaries along with the keystore.exe.config.ini file.
- CCD2/Contact Center Director — This directory contains contact center-related files.
- DBProvider — This directory contains database related files. The location of this directory is configurable during install.
- Email — This directory contains email headers that will be used for all emails being routed by the contact center.
- IVR — This directory contains IVR files.
- Log — This directory contains all logs. The location of this directory is configurable during install.
  - If you have installed and configured a Connect Edge Gateway device for use with Connect Contact Center, services logs are located on the Windows server where you host the virtual Edge Gateway in /var/log and are named <application>.access/error.log
- nginx — This directory contains nginx binaries and configuration files. ngnix is used by Connect Contact Center Director.

- Reverse Proxy — If you have installed and configured a Connect Edge Gateway device for use with Connect Contact Center, the following files are located as indicated:
  - conf.d — All contact center configuration files are under set6. For example: service_urls_set6_MCCC.conf. This file is populated by a configuration script provided by the Reverse Proxy team.
    The services covered in this configuration file are Web Agent, Contact Center Director, Contact Center API, and Chat.
    The following URL is configured for this services:
    - https://cc.shoretel.com (Web Agent)

Note

The Connect Contact Center Director cannot be accessed through Edge Gateway; it requires a VPN connection.

- Ruby — This directory contains Ruby binaries and configuration files. Ruby is used by Connect Contact Center Director.
- Web Agent — This directory contains two sub directories, which contain files related to the Mitel Interaction Center for the server and the client.
  - Server
    - Certs — This directory contains HTTPS certs.
    - Lib — This directory contains various javascript libraries used by the NodeJS Server. NodeJS is used by Web Agent.
    - Log — This directory contains WebAgent and External API logs.
    - Node_module — This directory contains NodeJS related files.
  - Client
    - Bin — This directory contains fonts, assets, Angular framework related files.

Installing the Connect Contact Center Software License Keys

Connect Contact Center ships with two types of software license keys: a system key and feature keys. The system key is required to run the Connect Contact Center system. The feature keys enable you to use specific Connect Contact Center features. These keys must be installed before you can use Connect Contact Center.

Connect Contact Center uses a system key. The system key you initially receive is not node-locked. You use this non node-locked system key to install and initially use Connect Contact Center. You then have 45 days to request and enter the required node-locked system key, while continuing to use Connect Contact Center. Refer to Requesting and Entering a Node-Locked System Key on page 39 for information.

Complete the following steps to install the Connect Contact Center software license keys:

1. From Connect Contact Center Director, click **Maintenance** > **License** > **License Keys** > **Add New License(s)**.
2. Copy the license information you received and paste it in the New License(s) field.
3. Click **Save**.

   The new license keys take effect immediately, and it is not necessary to restart or reboot Connect Contact Center.

Director Setup Prerequisites and Installing Supervisor Applications

Connect Contact Center supervisor applications can be installed either manually or through the active directory method that uses the Microsoft Installer (MSI). Manual installation involves downloading the software from the Mitel Support site and installing the software on each individual PC.

The active directory installation method simplifies deployments and reduces administrative costs. Connect Contact Center is configured, using the Windows Group Policy Object (GPO), to automatically push from the server to all computers in your call center. You must have Java installed on your supervisor machines for the Connect Contact Center supervisor applications to work after installation using the active directory method; and network connectivity is required during the installation process. To enable the active directory installation method, follow the instructions provided by MSI.

WARNING!

GPO push does not update the wecc.ini configuration file with the bootstrapping information the system uses to authenticate the supervisor system against the contact center server. System administrators must perform the steps in the Modify GPO Installer Database to Include Bootstrapper Information section to modify the GPO installer database so that the GPO push correctly updates the wecc.ini file with the bootstrapping information.

Modify GPO Installer Database to Include Bootstrapper Information

Launch the database editor of your choice (Mitel used Orca.exe) to edit the GPO installer database, modifying the following items in the Property table:

1. Set AUTHSERVERADDR to `https://<Mitel Connect headquarters server FQDN>/shoreauth`.
2. Set BOOTSTRAPSERVERADDR to `https://<Mitel Connect headquarters server FQDN>/shorestart`.

Mitel *strongly* recommends proceeding with caution while updating the GPO installer database to ensure that only these two values are modified.

Note

If you use the active directory installation method, and want to uninstall a Connect Contact Center supervisor application, you must uninstall using this same method (a GPO uninstall push).

Set up a Supervisor Administrator Account

Before you install supervisor applications on the supervisor system, you must set up a supervisor administrator in Connect Contact Center Director on the Contact Center server. This user role is necessary for accessing Connect Contact Center Director on the supervisor system.

Tip

Supervisors must log in to the Mitel Interaction Center before logging in to any other supervisor applications. Typical system configuration forces the supervisor to change their password upon initial login, and this procedure must be completed in the Interaction Center.

Notes

Supervisor records are tied to user records in the Connect PBX by **Client username**. The **Client username** configured for the agent in the Connect PBX must exactly match the **Username** configured here.

Complete the following steps to add a supervisor administrator account:

1. From Connect Contact Center Director, click **Supervisors** > **Accounts** > **New**.
2. In the **General** tab, specify the following:
   - **Name**
   - **Username** —This information must exactly match the **Client username** configured for this user in the Connect PBX.
   - **Sup COS** — The Supervisor Administrator will be assigned to the Standard COS.
3. (Optional) In **Agent Name**, choose an agent name for the supervisor.
4. In the Supervisor Permissions area, select Supervisor Administrator to configure this supervisor record to have permissions to modify system entities.
5. Click **Create**.

Configure Timezone Settings for Clients

In a Contact Center MiVoice Connect implementation, the time zone and Daylight Savings Time (DST) setting used by client applications, such as Agent Manager, should match the contact center server time zone and DST setting. To configure the client time zone and DST settings, navigate to the **System Parameters** > **Client Preferences** page in Connect Contact Center Director.

Manually Installing the Connect Contact Center Supervisor Applications

You can install the supervisor applications on multiple PCs; however, a license for each supervisor position is necessary for access to the applications.

Complete the following steps to install the Connect Contact Center supervisor applications:

1. Verify that the PC meets basic requirements, as specified in Chapter 2., Hardware and Software Requirements.
2. Request the installation files from a Mitel representative.
3. Connect the server to the network through the LAN adapter.
4. Turn on the supervisor PC.
5. Log into the system as a local administrator.
6. Navigate to the Mitel support site.download the Connect Contact Center installer, and then run the `setup.exe` file.
7. Click **Next** in the Welcome screen to continue.

   If you decide to stop the installation, click the **Cancel** button at any time throughout the process. If you want to return to the previous screen, click **Back**.
8. Accept the terms of the license agreement, and then click **Next**.
9. Enter the following information:
   - Authentication URL: https://<*Connect headquarters server IP address*>/shoreauth
   - Bootstrap URL: https://<*Connect headquarters server IP address*>/shorestart
10. In the Destination Folder screen, click **Next** to keep the default destination and continue the installation.

    The default destination is `C:\Program Files (x86)\ShoreTel\Contact Center`.

    Alternatively, you can click **Change** to locate and select a different destination folder, and then click **Next**.
11. In the resulting screen, click **Install** to begin installation of the software.

During the installation process, all files are installed into the appropriate directories. While the files are being installed, a status bar shows the progress of the process.

12. Click **Finish** to complete the installation process.

Troubleshooting Authentication and Bootstrapping

If there are any issues with this authentication, such as mistakenly entering the incorrect IP address for Connect HQ or needing to change the HQ IP address for any reason, complete the following steps:

1. Update all instances of the HQ IP address in the following files:
   - wecc.ini
   - WegAgentFramework.ini
   - EventAPI.ini
2. The wecc.ini file may need to be changed if an FQDN is used for the HTTPS certificate. By default, the wecc.ini file directs the system to use the IP address of the URL to log in. If an HTTPS certificate is used, this feature triggers browser errors or warning messages. The wecc.ini file must be manually changed to use the system domain name instead of the IP address.

   The following values in the CAC section of the wecci.ini file must be changed manually to show the domain name:

   - ECCServiceURI
   - CCD2ServiceURI

   For example,

   The wecci.ini file has the following IP address in the URL:

   ECCServiceURI=https://10.00.123.45:8433
   CCD2ServiceURI=https://10.00.123.45:31461

   Manually change this IP address as follows to show the domain name:

   ECCServiceURI=https://my.domain.name.com:8433
   CCD2ServiceURI=https://my.domain.name.com:31461
3. Restart the Connect Contact Center service.

Note

If you click the server icon on the desktop, the localhost in the URL is used, which causes a browser error or warning message if an FQDN is used with HTTPS. Use your domain name in https://my.domain.name.com/contactcenterdirector to login to the Connect Contact Center Director.

Starting and Verifying the Connect Contact Center Server

The Connect Contact Center Server software runs as service. When the Microsoft Windows OS starts, it loads and starts the Connect Contact Center Server service through the Windows Management Console.

Once you have started the server, you need to verify its operation. The Connect Contact Center Diagnostics Console is a powerful yet easy-to-use tool that provides a quick look at the operational status of the system with its main components.

To start Connect Contact Center Diagnostics Console, from the server select **Start** > **Programs** > **ShoreTel**> **ShoreWare Contact Center Server** > **ShoreWare Contact Center Diagnostics Console**. The Contact Center Diagnostics Console displays LEDs indicating the status of various system components. Each LED has three colors: red, yellow, and green. When the Automatic Call Distribution (ACD), IVR, and Private Branch Exchange (PBX) LEDs are green, the system is operational. The Chat and Email LEDs are yellow on systems that are not licensed for web chat or email. The online Help available from the Connect Contact Center Diagnostics Console provides details on the information displayed. For information about using the Connect Contact Center Diagnostics Console for advanced information on the system, refer to the *Mitel Connect Contact Center Administrator Guide*.

To properly shut down the Connect Contact Center Server, select **Start** > **Programs** > **Administrative Tools** > **Services**, and then click **Stop the ShoreTel Contact Center Service**.

Configuring Connect Contact Center for Interaction Reports (Optional)

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

Connect Contact Center provides interaction reports on inbound and outbound voice as well as email and chat activity including IRNs, IVR Port numbers, scripts played, and on the agent that answered the call. You must be a member of the Mitel Developer Network to receive documentation for the database schema and support for creating reports using this data.

Install CCIR on a server that is not running Connect Contact Center.

Note

Installing CCIR on a server that is running Connect Contact Center is *not* supported.

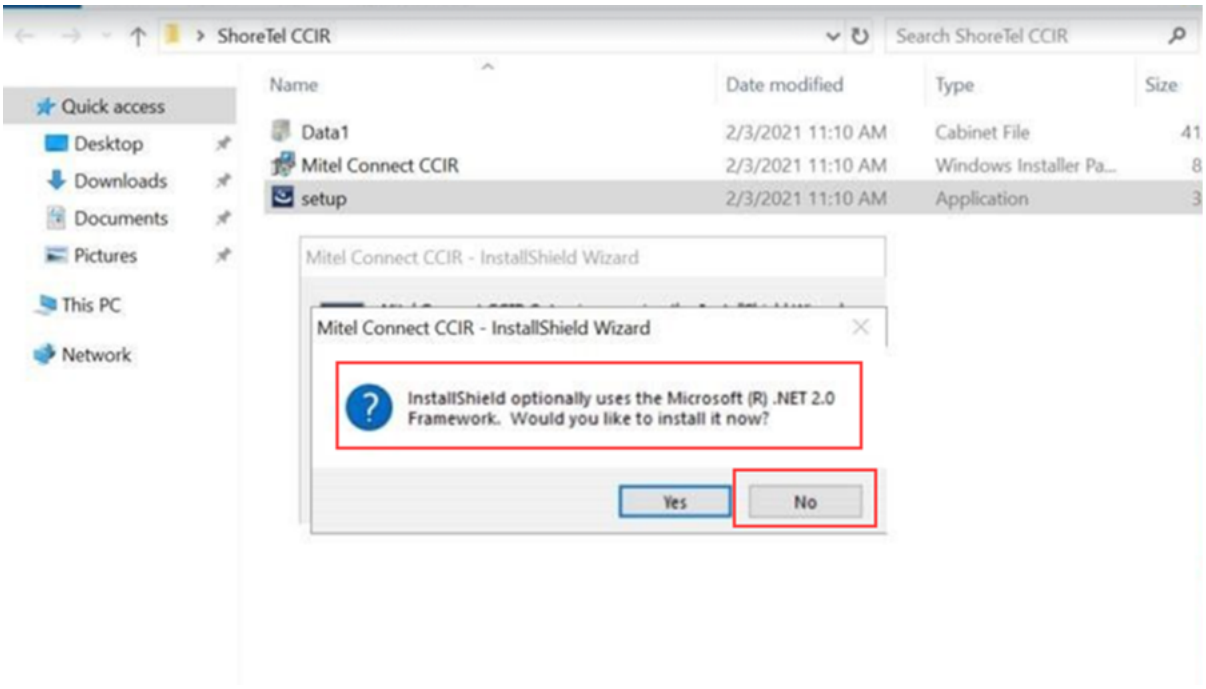
After configuring the Connect Contact Center system for interaction data, you can specify the call profile fields in the **System Parameters > External Interfaces > CCIR** page in Connect Contact Center Director. Data from these selected fields become the source of information in the reports. Refer to the *Mitel Connect Contact Center Administrator Guide* for information.

Adding a CCIR station

To add a CCIR station to the Connect Contact Center server, click `setup.exe` in the Mitel CCIR folder in the Connect Contact Center installation location and follow the prompts. Ensure the Primary Connect Contact Center Server is active.

Note

While installing CCIR on Windows Server 2019, the prompt **InstallShield optionally uses the Microsoft (R) .NET 2.0 Framework. Would you like to install it now?** appears. Click **No** to successfully install CCIR.



Adding a Secondary CCIR Station

1. Install a CCIR station on an external server by downloading the Connect Contact Center installation files, and then clicking `setup.exe` in the Mitel CCIR folder. Follow the prompts.
2. Ensure the Primary Connect Contact Center Server is active.
3. Configure the new CCIR station to be secondary CCIR in the **System Parameters** > **External Interfaces** > **CCIR** page of Connect Contact Center Director.
4. Wait for replication for finish.

When you add a new CCIR station, you must consider replication.

The new CCIR station is defined as a CCIR station that has not been replicated with any other CCIR stations in the same Connect Contact Center system and is a system that has just been configured as a secondary CCIR. Mitel does not recommend setting up a new CCIR station to be used as primary when there is already a working secondary.

When a new CCIR station, as defined above, is added, Connect Contact Center will try to replicate CCIR data from the existing CCIR station to the new CCIR station. Mitel recommends using a newly-built station with no CCIR data in it. However, if you use a CCIR station with existing data as a new CCIR station, the existing data will not be replicated to the other CCIR station. The existing data may, very likely, break the replication, if you are not familiar with how the replication works.

Refer to the *Rebuilding a Primary CCIR from Backup* and *Repairing CCIR Replications* sections of the *Mitel Connect Contact Center Administration Guide* for troubleshooting information about the CCIR.

Starting the Connect Contact Center Supervisor Applications

WARNING!

The Connect HQ server and the Connect Contact Center Server must be running before you can start a Connect Contact Center supervisor application. Do not start or run any of the supervisor applications from the Connect Contact Center Server. Supervisor applications should be used only on a supervisor PC. Running these applications on the server causes unexpected errors and results.

Before starting Connect Contact Center Director, ensure that JavaScript is enabled on your browser, and that the Connect Contact Center Director URL is accessible. This may mean that you need to add the Connect Contact Center Director URL to trusted sites in your browser. Refer to your browser documentation for information about how to do this. If JavaScript is not enabled, Connect Contact Center Director displays a warning.

Refer to Supported Browsers on page 17 for information about supported browsers.

Complete the following steps to start Connect Contact Center Director:

1. Enter the Connect Contact Center Director URL in your web browser's address field, as shown below:
   - If the HTTPS for Connect Center Clients is enabled during installation, use https://<*contact center server IP address or FQDN*>:8433/ccd.
   - Otherwise, use http://<*contact center server IP address*>:3000/ccd.

Note

Instead of the server IP address, you can use the name of the application server if a name resolution service or DNS is available. This is strongly recommended for if HTTPS is enabled to avoid browser errors and warnings.

Note

For information about handling insecure connection error messages on the browser, see the section *Browser warning message* in the *MiVoice Connect Contact Center Administration Guide*.

Tip

The wecc.ini file may need to be manually changed if an FDQN is used for the HTTPS certificate. For information about this, see Troubleshooting Authentication and Bootstrapping on page 35.

2. Enter your user ID and password in the **User ID** and **Password** fields.
3. Click **Submit**.

Complete the following steps to start the other Connect Contact Center supervisor applications:

1. From a supervisor PC, select **Start** > **Programs** > **ShoreTel**> **ShoreWare Contact Center Supervisor**, and then choose the application you want to open.
2. If this is your first time logging on to a supervisor application, specify your **Username** and **Password**.
3. Click **Login**.

Requesting and Entering a Node-Locked System Key

Connect Contact Center ships with a system key that is not node-locked. You then have 45 days to request and enter a node-locked system key while continuing to use Connect Contact Center. During this grace period, when you log into Connect Contact Center Director or any other supervisor application, a message is displayed specifying the number of days remaining.

Complete the following steps to request and enter a node-locked system key:

1. From Connect Contact Center Director, click **Maintenance** > **License** > **Request License**.
2. In the Request System Key page, type the requested information in the appropriate fields.

   Fields with a title in bold are required. The **Contact Email Address** is the email address to which the new license keys are to be sent.

   By default, the fields in the **System Values** area are automatically filled in with information from your Connect Contact Center Server. You should only change this information if you want a license for a server other than the one to which you are currently connected. If you have changed this information and want to restore default values, click **Restore Defaults**.

Note

If the **BIOS Serial Number** field is blank, either because the server does not have a BIOS serial number or it cannot be read, enter **NOBIOS** in the field.

3. Click Save. Then click Request. The information you entered is displayed, along with details on your currently licensed features.

4. To request your node-locked system key now, click **Request Online**.

   Your request for a system key is automatically sent to Mitel. The node-locked system key is sent to the email address you specified in the **Contact Email Address** field within 3 business days.

5. If you want to request your node-locked system key at a later, more convenient time, click **Print** or **Save Request**.

   Your request is displayed. Save this information as a text file. When you are ready to request the node-locked system key, send the file to licensekeyrequest@shoretel.com. The node-locked system key will be sent to the email address you specified in the **Contact Email Address** field within 3 business days.

6. Once you have received your node-locked system key, start Connect Contact Center Director and click **Maintenance** > **License** > **License Keys** > **Add New License(s)**. Copy the license information from the email and paste it in the **New License(s)** field.

7. Click **Save**.

   The node-locked system key takes effect immediately, and it is unnecessary to restart or reboot Connect Contact Center.

Installing the Ghostscript Component (Optional)

Supervisors can export historical reports to the PDF format. However, this feature is only available if the freeware component, Ghostscript, which is an interpreter for the PostScript language and for PDF, has been installed on the supervisor's machine.

Note

Use a user account that belongs to the operating system administrators group to install the Ghostscript component. This same user account must be configured for the printer account in the **Maintenance** > **Printer Account** page in Connect Contact Center Director.

You must use the same administrator account to install the Ghostscript component as you used to install the contact center system. Mitel *strongly* recommends that you use the operating system (OS) built-in administrator account to install the Ghostscript component. If you choose to not use the OS administrator account to install the Ghostscript component, and you install it using a different administrator account than the one you used to install the contact center system, you may encounter permissions issues that disrupt the distribution process involved in emailing reports from the contact center system.

If you encounter problems emailing reports, Mitel suggests you uninstall the Ghostscript component and reinstall it using the OS built-in administrator account.

The use of Ghostscript is subject to the terms and conditions of the GNU General Public License (GPL). Mitel suggests you review the GPL before installing Ghostscript.

Notes

- Before you install the Ghostscript component on a Windows 8 or Windows Server 2012 system, you must disable driver signature enforcement. Refer to the Windows documentation for information about this process.
- If you want to export scheduled reports to PDF format, you must also install Ghostscript on the contact center server while logged into Windows using the credentials defined in the Printer Account section of contact center Director. You define printer credentials on the **Maintenance** > **Printer Account** page in contact center Director.

Complete the following steps to install Ghostscript:

1. Download and run the `ghostscript 8.71` executable file for your operating system. Use `gs871w32.exe` for a 32-bit system and `gs871w64.exe` for a 64-bit system.
   The ghostscript executable file can be found in the Knowledge Base Article 000007484 "Ghostscript Driver for MiVoice Connect Contact Center".
2. In the Self-Extractor window, click **Setup**.
3. Modify installation options as necessary, and then click **Install**.
4. When installation is complete, choose **File > Add Printer** from the Windows **Settings** > **Printers and Faxes**.

5. Using the Add Printer Wizard, select the **Local Printer Attached to this Computer** option, and then select the port **FILE: (Print to File)**.
6. In the Install Printer Software window, click **Have Disk**. In the resulting window, click **Browse** to locate and select the `ghostpdf.inf` file.

   The default location of the ghostscript.inf file is `C:\Program Files (x86) \gs\[version]\lib`.
7. Click **Open**, and then **OK**. The Ghostscript PDF printer is displayed in the Printers list.
8. Click **Next**.
9. In the Name Your Printer window, enter **Sybase Datawindow PS** in the Printer Name field. You must enter this printer name exactly as indicated or the feature will not work.
10. Follow the prompts through the remainder of the Add Printer Wizard. The Sybase Datawindow printer appears in the Windows Printers and Faxes window.

Installing Distributed IVR Servers (Optional)

Distributed IVR servers can be used to scale the system to more agents and to minimize WAN bandwidth utilization. The IVR or media servers perform the functions of playing queued music, announcements, or self service modules. Distributed IVR servers are managed by the main Connect Contact Center Server, which distributes the load between the multiple IVR/media servers if more than one server is used.

IVR ports are used by Connect Contact Center to perform an IVR action on a call, and are supported on both the Connect Contact Center server and IVR servers (such as an existing DVS server). IVR software can run on a DVS as long as the total media ports used is not more than 250. There is no software based restriction to prevent you from over provisioning. IVR ports on a secondary server (for redundant configuration) running as slave are not utilized until the secondary server becomes the master.

An IVR port is considered local to a call only when the other end of the call is on the same site as the IVR port. An IVR port is considered remote to a call if the other end of the call is on a different site, or the site information cannot be determined. For inbound calls, the concept of local is relative to each call. One call's local IVR port can be a remote IVR port for another call.

The system selects an IVR port based on the following rules:

- **Rule 1** — Whenever an IVR port is needed for an incoming call, the Connect Contact Center system tries to first assign a local IVR port. If no local IVR port is available, a remote IVR port is assigned. If local IVR resources exist, but are being used for a particular call, the system logs an event indicating the site has insufficient IVR resources for the call.
- **Rule 2** — If more than one server has ports available and they are equal (i.e. the ports are all local or all remote), then the IVR ports from the server with lower proportional utilization is selected.

Each IVR port has its own license in Connect Contact Center. You need an IVR port license for every IVR port configured in the system. A call is connected to an IVR port whenever a call is waiting in a queue or being serviced by a call control script (CCS) or announcement.

The procedure described here is for standalone installations only.

Complete the following steps to install a distributed IVR server, on the IVR station machine:

1. Install the Distributed Voice Server (DVS).
2. Configure the route points that you will use as IVR ports. (IVR Route Points hosted on a distributed IVR workstation must be configured so that the Route Point Server configured within the Route Point has the distributed IVR workstation selected).
3. Install the IVR station by clicking the `setup.exe` file in the Connect Contact Center IVR folder in the installation location. After installation, restart the Connect Contact Center Server. Refer to Installing the Connect Contact Center Server on page 25 for more information.
4. On the Connect Contact Center Server, start Connect Contact Center Director. Then from **IVR Configuration** > **Route Points** > **IVR Ports**, add a new IVR port. This process is described in the *Mitel Connect Contact Center Administrator Guide*.
5. Copy all wave files from the Primary server to all IVR stations using the **Maintenance** > **File Replication** > **Replicate Now** page in Connect Contact Center Director.

Installing and Configuring Nginx Proxy on a Redundant System

For a system with redundancy, you can configure the Nginx proxy to use the Distributed database servers to enable agents log in to the Interaction center through the AIC portal when the HQ server is offline.

In the Connect Contact Center redundant server system, the operational server is backed up by a secondary server. The secondary server can run as a remote server on a separate network segment. For more information about a redundant system, refer to Implementing the Redundant Server System chapter in the *Mitel MiVoice Connect Contact Center Administration Guide*

Prerequisites

- Redundant system with primary and secondary servers.
- The primary and secondary servers have the local Distributed Database Server enabled on the HQ Server. To enable the Distributed Database Server on HQ server, refer to the Mitel Distributed Database section in the *Mitel Connect System Administration Guide*.
- The primary and the secondary servers are installed with a proxy server IP address specified as the Authentication and Bootstrap URL.
- Trusted sites.

System Specifications

- Operating System – CentOS Linux release 7.4.1708 (Core)
- Nginx Version – nginx/1.12.2
- Host Type – VMWare 6.5

Installing and Configuring the Nginx Proxy

To install and configure the Nginx Proxy on a CentOS virtual machine:

1. In the command prompt, run the command `sudo yum install epel-release` to add the Nginx repository to the system.
2. Install and enable the Nginx proxy respectively using the following commands:

   ```
   sudo yum install nginx

   sudo systemctl enable nginx
   ```

3. Download the **proxy.zip** file to the CentOS machine from https://oneview.mitel.com/s/article/Mitel-Connect-ONSITE-Contact-Center-Software.
4. Unzip the downloaded file as follows:

   ```
   # unzip proxy.zip
   Archive:  proxy.zip
   creating: proxy/
   inflating: proxy/proxy_config.rb
   extracting: proxy/proxy.sh
   inflating: proxy/nginx.conf
   inflating: proxy/nginx_dds_proxy.template
   extracting: proxy/proxy.zip
   inflating: proxy/README.txt
   ```

5. Change the directory to **proxy** by using the command, `# cd proxy`.
6. Run **bash proxy.sh** in the **proxy** directory as a sudo user. Enter the IP addresses of the current server on which the proxy is running, HQ server, and primary and secondary servers respectively.

   ```
   # bash proxy.sh
   please enter the current server address - the server you are running the reverse
   proxy
   10.23.137.11
   please enter the HQ server address
   10.23.137.12
   please enter the primary server address
   10.23.137.24
   please enter the secondary server address
   10.23.137.26
   server ip is: 10.23.137.11
   hq ip is: 10.23.137.12
   ```

```
primary ip is : 10.23.137.24
secondary ip is : 10.23.137.2
```

7. Confirm if the **nginx.conf** file is generated as shown:

```
# ls -atlrh
total 28K
-rw-rw-r--.  1 admin admin  837 Mar 23 06:37 proxy_config.rb
-rwxrwxr-x.  1 admin admin   34 Mar 23 06:37 proxy.sh
drwx------. 16 admin admin 4.0K Mar 23 06:37 ..
-rw-r--r--.  1 admin admin 4.2K Mar 23 06:40 nginx_dds_proxy.template
drwxrwxr-x.  2 admin admin   95 Mar 23 06:40 .
-rw-r--r--.  1 root  root  4.3K Mar 23 06:40 nginx.conf
```

8. Copy the generated file to the **/etc/nginx.conf** location:

```
 #cp nginx.conf /etc/nginx/nginx.conf
```

9. Type **y** for the command, `cp: overwrite ‘/etc/nginx/nginx.conf’?` to overwrite the existing nginx.conf file.

10. Check for any errors in the configuration as shown:

```
# sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

There should not be any errors, and the message **nginx: configuration file /etc/nginx/nginx.conf test is successful** indicates a successful configuration.

11. Reload the new Nginx configuration. You will not be prompted with any output.

```
# nginx -s reload
```

Upgrading the Redundant System and the Supervisor Client

1. Upgrade the primary and the secondary server systems. When prompted to specify the Authentication and the Bootstrap URL, specify the Nginx proxy server over http as follows:

   - Authentication URL: http://<proxy-ip>/shoreauth
   - Bootstrapper URL: http://<proxy-ip>/shorestart

   For more information about upgrading the servers, refer to Upgrading a Redundant System (Optional) on page 71.

2. Upgrade the Supervisor client. When prompted to specify the Authentication and the Bootstrap URL, specify the Nginx proxy server over http as follows:

   - Authentication URL: http://<proxy-ip>/shoreauth
   - Bootstrapper URL: http://<proxy-ip>/shorestart

   For more information about upgrading the client application, refer to Upgrading Client Applications on page 72.

3. If the configuration is successful, you can now use the Nginx proxy server to log in to the AIC and the CCD2 directories. Use the following URLs to log in to the AIC and CCD2 portals respectively:
   - http://<proxy-ip>:8080/MCCC
   - http://<proxy-ip>:8080/ccd2

Tip

For the IP addresses, refer to Installing and Configuring the Nginx Proxy on page 44.

4. If the authentication is successful, you are redirected to the landing page of the active/primary server system.
5. Start the Supervisor Client application and confirm if you can log in to the Agent Manager or GCCS.

   Optionally, you can also confirm if the installation and the configuration of the Nginx Proxy is successful by verifying the following:
   - When the HQ server is offline, and the primary server is active, agents can log in to the AIC portal over the proxy and take new calls.
   - When the HQ server is offline, and the Failover mode happens, the secondary server should be running. For more information about the Failover mode, refer to the Failover Mode section in the *Mitel MiVoice Connect Contact Center Administration Guide.*

Troubleshooting Databases not in Sync between HQ and Primary and Secondary Servers

If the PBX databases of the primary and the secondary servers are not in sync, you can sync them through the Mitel Connect Director.

1. Open the Mitel Connect Director.
2. Click **MAINTENANCE** > **Status and Maintenance** > **Servers**.
3. In the **Servers** field, under the **DB** tab, the icons for the primary and the secondary servers are red in color, if the databases are not in sync.
4. To sync the databases, click **RESYNC DATABASE**. The databases are synced and the icons on the **DB** tab will appear green in color.

Uninstalling Connect Contact Center

The process for uninstalling Connect Contact Center involves removing the server, the database directories, and the client applications from your machines.

If you originally used the active directory installation method to install the Connect Contact Center supervisor applications, and you want to uninstall a supervisor application, you must uninstall using this same method (a GPO uninstall push).

Note

When Connect Contact Center is uninstalled, the database remains untouched. You can make a copy of this database and store it elsewhere to access later, or you can delete the database as part of the uninstall process.

Uninstalling the Connect Contact Center Server and Database Directories

Complete the following steps to uninstall the Connect Contact Center server and database directories:

1. From the Control Panel, select **Add or Remove Programs.**
2. Select **ShoreTel Connect Contact Center Server Software**, and then click the **Change/Remove** button.

   All server software components, excluding the database directory, are removed from your system.
3. Manually delete the database directory **DbProvider** from your system.

   The directory is located on your system where Connect Contact Center was previously installed.

   Your server is now ready for a new installation of Connect Contact Center Server.

Manually Uninstalling the Connect Contact Center Client Applications

Complete the following steps to manually uninstall the Connect Contact Center client applications:

1. From the Control Panel, select **Add or Remove Programs.**
2. Select **ShoreTel Connect Contact Center Supervisor** or **ShoreTel Connect Contact Center Agent**, and then click the **Change/Remove** button.

   All client software components are removed from your system, and the computer is ready for a new installation of the Connect Contact Center client applications.

Using the Installation Logs to Diagnose Problematic Installations

The purpose of an installation log is to assist in troubleshooting problematic installations. It helps in troubleshooting by showing information to the Mitel administrator. The administrator can communicate this information to Mitel TAC to accelerate the resolution of the problem.

During an installation, the system creates a log that is specific to each Connect Contact Center application. For example, installation of the server software or the supervisor software creates a unique log.

After a successful installation or just an attempted installation of an application, the log for the application resides in the folder that contains the application. The identification of the log is by date, which is in YYYYMMDD format, time stamp in 24-format, and the string “Install.” The format of the installation log is *date_time*_Install.txt

A sample log file name is `20120601_1338_Install.txt`.

The format of the log file’s name does not identify the application. However, the location of the file and certain contents of the file do identify the application. The location and contents in the following example show a supervisor installation:

```
C:\Program Files (x86)\ShoreTel\Contact Center\Supervisor\20120530_0749_Install.log
```

Note

The example screens do not show errors, only successful installations. If a task fails, the display shows that this task is where the installation stopped. Mitel TAC uses this information to diagnose the problem.

The following figure shows that this log is for a supervisor installation. It also shows the build number for the software.

07:49:35AM Operating system: Microsoft(R) Windows(R) Server 20xx, Enterprise Edition Service Pack 2
07:49:35AM The Windows Firewall is disabled
07:49:35AM Install location: C:\Program Files (x86)\ShoreTel\Contact Center\Supervisor
07:49:35AM Free Disk space: 0.4GB
07:49:35AM This is a fresh install of the ShoreTel Contact Center Supervisor.
07:49:35AM Executed InstallShield Custom Action CostInitialize
07:49:36AM System IP address: 10.1.3.255
07:49:36AM Installing ShoreTel Contact Center Supervisor Version: 505.5.5800.0
07:49:36AM Could not determine server IP address.
07:49:36AM Executed InstallSheild Custom Action InstallValidate
07:49:37AM This is not a Pre-Draco upgrade installation.
07:49:38AM Executed InstallSheild Custom Action RegisterExtensionInfo
07:49:41AM Executed InstallSheild Custom Action InstallInitialize
07:49:45AM Executed InstallShield Custom Action StopServices
07:49:56AM Executed InstallSheild Custom Action CreateFolders

For the next example, the log of the server installation resides in the default location. The log for a server installation contains more information than other installation logs:

```
C:\Program Files (x86)\ShoreTel\ ShoreTel Contact Center
Server\20120601_1338_Install.log
```

In the example of a partial log file in the next figure, the log contains the version of Mitel system software with which the Connect Contact Center server inter operates, the type of application (Connect Contact Center server), and the build number of the server software.

```
01:38:03PM Operating system: Microsoft(R) Windows(R) Server 20xx, Standard Edition Service Pack 2
01:38:03PM The Windows Firewall is disabled
01:38:03PM ShoreWare Server version found: 14.5.5404.0
01:38:03PM Install location: C:\Program Files (x86)\ShoreTel\ShoreTel Contact Center Server\
01:38:03PM Free Disk space: 10.4GB
01:38:03PM DBProvider folder size: 107.3MB
01:38:03PM Previous installation of ShoreTel Contact Center Server 504.7.8002.0 found.
01:38:03PM Executed InstallShield Custom Action CostInitialize
01:38:03PM Executed InstallShield Custom Action FileCost
01:38:03PM Executed InstallShield Custom Action CostFinalize
01:38:03PM System IP address: 10.17.10.101
01:38:03PM Installing ShoreTel Contact Center Server Version: 505.5.5800.0
01:38:03PM Executed InstallShield Custom Action MigrateFeatureStates
01:38:11PM Executed InstallShield Custom Action InstallValidate
01:38:12PM Backup of wecc.ini file created.
01:38:12PM Executed ShoreTel Custom Action StartMySQLonInstall
01:38:12PM ShoreTel Custom Action StartMySQLonInstall: ShoreTel-MySQLCC service is running.
01:38:14PM A database schema upgrade is required
```

A fresh install or an upgrade process logs an entry after executing each installer action that InstallShield generates. Example actions would be CreateFolder or MoveFiles. If the system has to roll back during a fresh install or upgrade, the records for the installer's rollback actions go to the same log file.

The difference between a fresh install and upgrade install are negligible. The additional details in an upgrade log show:

- That it is an upgrade install.
- Whether a database schema upgrade is needed.
- That the system copied the DbProdiver directory to DbProvider.upg as well as the results of a folder comparison.
- The creation of the MySQLupg service.

CHAPTER

4

Setting Up Connect Contact Center

This chapter includes information about setting up Connect Contact Center in the following sections:

Integrating Connect Contact Center with the Mitel System

The Mitel system and the Connect Contact Center Solution connect by way of a software interface in an IP network. This interface conforms to the industry-standard Telephone Application Programming Interface (TAPI) and allows the system and application to exchange call control information. It also allows interaction with audio play files and can respond to a caller's keypad input.

The Mitel system interfaces to Connect Contact Center are:

- **Destinations** — Dialable extensions in the Mitel system configured as route points that deliver calls to the Connect Contact Center intelligent routing numbers (IRNs).

- **IVR Ports** — An interface between callers and interactive voice response (IVR) scripts, which are configured as route points in the Mitel system. IVR ports support caller interactions and connect a caller to music or announcements while waiting in queue.
- **Agent Extensions** — Normal extensions in the Mitel system that an agent has in a call center. Agent extensions are monitored by Connect Contact Center to make routing decisions and for reporting.

This chapter assumes that you have successfully installed:

- Mitel Distributed Server software
- Connect Contact Center Server software

In addition, the Connect Contact Center Diagnostics Console must display green LEDs for the ACD, IVR, and PBX, as explained in Chapter 3., Installing Connect Contact Center.

To integrate Connect Contact Center with a Mitel system, a system administrator must be familiar with Mitel system requirements and administration. For more information, refer to the current *Mitel Planning and Installation Guide* and the *Mitel System Administration Guide*.

Identifying Server Route Points

Route points enable calls to be terminated and controlled in the network by the Connect Contact Center Server.

Complete the following steps to identify server route points:

1. Create route points for Connect Contact Center Intelligent Routing Numbers (IRNs)
2. Create route points for Connect Contact Center interactive voice response ports (IVRs)

An IRN is a route point for the incoming calls that are directed to the Connect Contact Center Server software. With these route points, Connect Contact Center has complete access to call control signaling by using TAPI and the actual voice media stream by using TAPI and wave APIs.

The Connect Contact Center Server software uses IVRs are used to transmit queue messages, prompts, and music-on-hold to callers who are connected to the Connect Contact Center through the Mitel system.

Note

Do not assign IPBX schedules to IRN route points unless the Route Point Server is the Headquarters server or a ShoreWare Distributed Server that has the Allow Voice Mailboxes option enabled. The Distributed Server that the Contact Center software is installed on should *not* have this option enabled.

Creating IRN Route Points on the Connect PBX

Create a route point for each IRN port, as follows:

1. Launch Connect Director and log in as an administrator.
2. Navigate to the **Administration** > **Features** > **Call Control** > **Route Points** page.
3. Click **New**, and enter the following information:
   - **Name** — The descriptive name of the IRN route point, such as Sales_IRN.
   - **Extension** — The extension number of the route point. Each route point extension must be unique. Any calls sent to this extension are routed to a corresponding IRN defined on the Connect Contact Center Server.
   - **User Group** — From this drop-down menu, assign a user group to the route point. Select **Executives User Group**, which has the appropriate Class of Service with full features.
   - **Route Point Server** — From this drop-down menu, select the appropriate server. On a nonredundant system, the Route Points must be configured on the Distributed Server where the Contact Center Server software resides. If the route point has an IPBX schedule, then you must select the Headquarters or a DVS with mailboxes enabled.
   - **Mailbox Server** — The server that hosts the mailboxes. Select the check box to enable the drop-down, and then select the appropriate server in the drop-down list. Ensure you do not select the Connect Contact Center server from the drop-down list.

Tip

If the **Administration > Appliances/Servers > Platform Equipment > Voice Application > Allow Voice Mailboxes** option is not selected for the Headquarters or DVS server in Connect Director, the Connect Contact Center server is not included in the **Mailbox Server** drop-down list.

   - **Call Stack Depth** — Set the Call Stack Depth to 30. With this feature, you can specify the maximum number of simultaneous calls that can be stacked on the route point extension. When this number is met, additional inbound calls will be routed to the call forward busy destination.
   - **Call Forward** — These buttons enable you to specify when calls are forwarded after the specified number of rings or when the call stack is full. The conditions are **Always**, **No Answer/Busy**, and **Never**. Select **No Answer/Busy**.
   - **Busy Destination** — When the **No Answer/Busy** call forward condition is selected, calls are forwarded to this extension immediately if the user's call stack is full. You can also forward calls to an external number. An access code is required for this function.
   - **No Answer Destination** — When the **No Answer/Busy** call forward condition is selected, calls are forwarded to this extension after the specified number of rings. You can also forward calls to an external number. An access code is required for this function.

- **No Answer Number of Rings** — When the **No Answer/Busy** call forward condition is selected, this option specifies the number of times the phone rings before the call is forwarded to the No Answer Destination.

4. Click **Save**.

   Repeat this procedure for each IRN and IVR port that you want to create.

IRN Route Point Limitations

Calls directed to IRN Route Points are limited to the following routing scenarios:

- DNIS map from a Trunk Group to a Connect Contact Center Route Point
- DID assigned on a Connect Contact Center Route Point
- Programming a transfer-to-extension or go-to-extension operation from an auto attendant directed to a Connect Contact Center Route Point
- User-blind or consultive transfer to a Connect Contact Center Route Point

Tip

Analog devices must be blind transferred to contact center. Consultative transfers from an analog device will not complete.

Forwarding a Call

Complete the following steps to forward a call from a non-Connect Contact Center Route Point, Workgroup, Hunt Group, or a user's personal call handling mode:

Tip

Forwarding a call in this scenario also includes the use of the **No Answer**, **Busy**, or **Backup** destinations. Do not use a Connect Contact Center Route Point extension as a Workgroup or Hunt Group member. Refer to KB16764 on www.shoretel.com/support for additional information.

1. Create an Auto Attendant with the Time out variable programmed with the Transfer to extension or Go to extension operation that is directed to the Connect Contact Center Route Point.
2. Record the prompt with a second or two of silence, otherwise the system prompt for a basic Auto Attendant will be played, which might confuse the caller.
3. Reduce the default Timeout value from 8000 ms to 2000 or 3000 ms. Do not reduce the Timeout value to 0 or 1 ms to ensure the Auto Attendant answers and transfers the call instead of forwarding the call.
4. All other Operations for the Auto Attendant can be set to <None>.

Creating IVR Route Points on the Connect PBX

Each IVR port must have a configured route point.

Setting up IVRs is similar to IRNs. The main difference between IVRs is that IRNs can have a call stack of 16. Each caller that reaches the Connect Contact Center has one IVR. Therefore, enough IVRs must be available for the call volume. IVRs are available across all groups and not confined to a particular call group. For example, Sales and Customer Support do not have separate IVRs.

Complete the following steps to create an IVR route point:

1. Launch Connect Director and log in as an administrator.
2. Navigate to the **Administration** > **Features** > **Call Control** > **Route Points** page.
3. Click **New**, and enter the following information:
   - **Name** — Type a descriptive name for the IVR route point—such as **IVR-01**, **IVR-02**, and so forth.
   - **Extension** — This is the extension number of the route point. Each route point extension must be unique. No calls are dialed into IVR extensions. The extensions are used only for calls originating from the Connect Contact Center Server. Mitel recommends that you use extensions to help manage the IVRs.
   - **User Group** — From this drop-down list, assign a user group to the route point. Select **Executives User Group**, which has the appropriate class of service with full features.
   - **Route Point Server** — Select the ShoreWare Distributed Server where the Contact Center Server software resides.
   - **Mailbox (server)** — Ensure that this check box is **not** selected.
   - **Call Stack Depth** — Set the Call Stack Depth to **1**. You cannot stack calls on an IVR route point.
   - **Call Forward** — Use to specify when calls are forwarded after the specified number of rings or when the call stack is full. The conditions are **Always**, **No Answer/Busy**, and **Never**. Select **Never**.
4. Click **Save**.

   To configure another IVR route point, click **Copy,** and then type a new name and extension for the new IVR route point.

Configuring Email

Note

If you use Office 365 and your call center has the potential to receive 30 or more emails a minute, you must configure your MCCC server to be an SMTP relay. This configuration will ensure that your call center does not have issues receiving emails. For information about how to configure your MCCC server to be an SMTP relay, visit https://technet.microsoft.com.

Configuring email provides the ability to route customer email to call center agents. Agents can receive customer emails and then respond with a solution. Routing email through Connect Contact Center provides detailed reporting on email flows and the overflow and interflow routing of emails.

Connect Contact Center functions as an email client of your corporate mail server. As an email client, Connect Contact Center receives customer email for distribution to agents. Agents that are logged into Mitel Interaction Center and belong to a email group are notified of an available email. When the agent clicks the Answer button in Mitel Interaction Center, the agent receives an email from the Connect Contact Center server. When an agent replies to a customer email the reply email is routed to the reply email account, which is monitored by Connect Contact Center. On receipt of the reply email Connect Contact Center will automatically terminate the agent interaction and forward the reply to the customer.

The Mitel corporate email servers manage reception and transmission of Connect Contact Center email, providing the following features:

- Handling of a dead letter archive
- Email groups
- Individual agent email
- Pre-defined responses that appear to be communicated directly by an agent
- Routing of high priority emails
- Single-click to answer an email
- Re-routing of emails that agents answer but to which they do not respond
- Reporting for the time between answer and reply or hang-up by agent
- Cradle-to-grave reporting

Email Requirements

This section describes the requirements for the corporate email server to provide email services to Connect Contact Center agents and callers whose email goes to Connect Contact Center.

Permitting Connect Contact Center to Respond to Email Contacts

If a Connect Contact Center customer allows agents to respond to caller emails by sending a generic response, such that the sender is always a customer-specified name and the identity of the agent is hidden, the company's network security implementation must allow Connect Contact Center to perform this type of email transmission. Default anti-virus settings might block the outbound email transmission from the Connect Contact Center server, so change these settings in the anti-virus software as needed to permit outbound emails.

Corporate Mail Server Requirements

In addition to the general system requirements to install and run a corporate mail server, the mail server software must meet the following requirements for Connect Contact Center email:

- **IMAP4 Support** — Connect Contact Center uses IMAP4rev1 to retrieve emails from the corporate mail server. The default port is 993 if the connection is encrypted (SSL) or port 143 without encryption. In the current release, the Connect Contact Center email subsystem uses only IMAP4rev1.
- **SMTP Support** — The corporate mail server must support SMTP for outgoing mail. The default port is 25.

Ports	Protocol	Usage	Encryption
993	IMAP	Incoming	SSL
465, 587	SMTP	Outgoing	StartTLS

Configuring the Corporate Mail Server

Refer to the following sections for information about configuration to complete on the corporate mail server.

Read Receipt Configuration

To manage read receipts, configure the mail server to suppress read receipts. For example, for Microsoft Exchange Management Shell, you might specify set-ImapSettings -SuppressReadReceipt $true. Refer to the documentation for your mail server for detailed information about suppressing read receipts.

Mailbox Configuration

The mail server must have a mailbox for each email address that Connect Contact Center uses. Add email accounts for the following:

- The accounts Connect Contact Center will receive customer emails at, for example sales@shorebank.com and support@shorebank.com. These accounts can also be on different mail servers, for example customersupport@gmail.com.
- The reply account agent replies are routed through, for example ccreply@shorebank.com

- The dead letter account, for example dead-letter@shorebank.com

Configuring the Agent's Email Address

The Connect Contact Center administrator configures the email address for every agent that is member of an email group.

Preparing Agent Phones

The Connect Contact Center Solution supports agents who use only a telephone. Agents using phones can perform the following Automatic Call Distribution (ACD) management activities:

- Log in to and out of primary groups
- Release
- Resume

When phone-only agents are logged on, they receive calls as defined by the routing policy and are monitored as regular agents by the Connect Contact Center supervisor applications.

Note

Connect Contact Center does not support more than two calls on an agent telephone at the same time.

To prepare the phone-only agent positions, define four specific Intelligent Routing Numbers (IRNs) using Connect Contact Center Director > **Routing** > **IRN**. Each IRN must have a default destination or a predefined ACD interactive voice response (IVR) Script.

The ACD actions are performed by dialing the IRN Dial Number and following the instructions.

Selecting the Data Sources used by ODBC Connections

The Connect Contact Center system uses information from an external database to direct the routing of calls in call control scripts, in dial lists, and for other functions. The system relies on Open Database Connectivity (ODBC) to support the API for accessing external databases.

Part of the process of configuring an external database connection is to set up the data sources used by your ODBC Connections. Refer to the *Mitel Connect Contact Center Administrator Guide* for details.

Configuring the Database Connection

Configure an ODBC database connection, as follows.

1. From the **Control Panel** > **Administrative Tool** > **Data Sources (ODBC)** > **System DSN** tab, select the appropriate driver to add a new connection.

Note

For a Connect Contact Center server on a 64-bit system, run `\SysWOW64\odbcad32.exe` and select the appropriate driver to add a new connection in the DSN tab. The executable `odbcad32.exe` applies to 64-bit and 32-bit systems.

2. Click **Configure**.
3. Create the database connection in Connect Contact Center from Connect Contact Center Director **> System Parameters** > **External Interfaces** > **Database Connections**.
4. In the **General** tab, specify the appropriate information for the connection, and then click **Save**.

Refer to the *Mitel Connect Contact Center Administrator Guide* for additional information about creating the database connection.

Preparing to use Interaction Reports and Event Feeds (Optional)

Note

CCIR is included for third-party products to enable and maintain the existing integration. Contact the respective service providers for any questions about interoperability on third-party products. Contact Mitel Advanced Application team for issues related only to CCIR or CCIV. Mitel Technical Assistance Center (TAC) does not support on issues related to CCIR, CCIV or third-party products.

Connect Contact Center Interaction Reports (CCIR) and Event Feeds provide additional data on call center activities.

CCIR reports on inbound and outbound voice as well as email and chat activity including IRNs, IVR Port numbers, scripts played, and on the agent that answered the call. If your organization plans to use CCIR, you need to do the following:

1. Contact the Mitel Developer Network to receive documentation on the database schema and support on creating these reports.
2. If you prefer to have the information stored on an external machine, you can specify an external installation.
3. Specify the CCIR parameters using Connect Contact Center Director, as explained in the *Mitel Connect Contact Center Administrator Guide*.

Event feeds allow your organization to access information, through the implementation of an API, on agent and group activity using third-party applications. If your organization plans to use event feeds, you need to do the following:

1. Contact the Mitel Developer Network to receive documentation and support on the APIs.

Specify the credentials of the connecting application using Connect Contact Center Director. This process is explained in the *Mitel Connect Contact Center Administrator Guide.*

CHAPTER

5

Testing Connect Contact Center

After configuring Connect Contact Center, you need to test the system to ensure that Connect Contact Center is installed properly and operating correctly. Testing involves the creation of the basic components of the system by using Connect Director and Connect Contact Center Director and then verifying that calls are received and correctly routed. For detailed information on using Connect Contact Center Director, refer to the *Connect Contact Center Administrator Guide*.

Refer to the following sections for more information about testing Connect Contact Center:

Creating a Supervisor Account

Supervisors are responsible for specific groups of agents. They monitor agent performance and call center activities. Each supervisor receives permissions that allow or prevent access to system operations.

Note

Supervisor records are tied to user records in the Connect PBX by Client username. the Client username configured for the agent in the Connect PBX must exactly match the **Username** configured here.

Complete the following steps to add a supervisor account:

1. From Connect Contact Center Director, click **Supervisors** > **Accounts** > **New**.

   If you have an existing supervisor account with parameters similar to what you want, you can quickly create a new account by clicking **Copy**.

2. In the **General** tab, specify the following:

   - **Name**
   - **Username** —This information must exactly match the Client username configured for this user in the Connect PBX.
   - **Sup COS** — The Sup COS is a supervisor class of service that specifies supervisor capabilities. Refer to Creating a Supervisor Account on page 59 for information about setting up this COS.

3. In **Agent Name**, choose an agent name for the supervisor.

   The agent names in the menu have been previously defined. Refer to Creating an Agent Account on page 60 for details.

4. In **Alert Type**, choose the audio alert the supervisor hears when a a real-time group report reaches or exceeds a threshold.

   The alerts in the menu have been previously defined. Refer to the Defining Supervisor Alerts section of the *Connect Contact Center Administration Guide* for information.

5. In the Supervisor Permissions area, select the appropriate permissions for the supervisor:

   - **Supervisor Administrator** — Access and modify system entities.
   - **Entity Administrator** — Access and modify all system entities except supervisor accounts.
   - **Entity Monitor** — Access specified Connect Contact Center reports.

6. Select **View Real-Time Reports (Agent Manager)** to allow the supervisor to view and update real-time reports using Agent Manager.

7. Click **Create**.

Creating an Agent Account

Agents handle contacts routed to them by the Connect Contact Center Solution. Each agent is equipped with a telephone, and begins work by logging into the system.

Note

Agent records are tied to user records in the Connect PBX by Client username. the Client username configured for the agent in the Connect PBX must exactly match the Agent Username configured here.

Complete the following steps to create an agent account:

1. From Connect Contact Center Director, click **Agents** > **Agents**.
2. Click **New**.

   If you have an existing agent account with parameters similar to what you want, you can quickly add a new account by selecting it and clicking **Copy**.
3. In the **General** tab, specify the following:

   - **Agent Name**
   - **Agent Username** —This information must exactly match the Client username configured for this user in the Connect PBX.
   - **Agent ID**
   - **Agent Extension**
4. New agents are automatically assigned the COS Standard Agent. Refer to the Defining a Class of Service section of the *Connect Contact Center Administration Guide* for information about the default parameters of this COS. If you want to assign a different COS to the agent, select it from the **Class of Service** drop-down menu.

Note

If your system includes agents defined in older versions of MCCC, those agents they will be assigned to the Default COS, which has all COS features enabled by default.

5. If you want to assign an agent queue profile to the agent, choose the profile from the **Agent Queue Profile** drop-down menu.

   You must define Agent Queue Profiles before adding them to agent records. See the *Creating Agent Queue Profiles section* of the *Connect Contact Center Administration Guide* for more details.
6. If you want to assign an email agent queue profile to the agent, choose the profile from the **Email Agent Queue Profile** drop-down menu.

   You must define Email Agent Queue Profiles before adding them to agent records. See the *Defining Email Agent Queue Profiles section* of the *Connect Contact Center Administration Guide for more details*.
7. Specify the **Email Address** used by the system to route email contacts to the agent's email address, which is typically the agent's corporate email address.
8. Select **Auto Answer Incoming ACD Voice Calls** to direct the system to answer calls to this agent if the agent does not answer after one ring.

9. Select **Forced Wrap-Up** to require the agent to enter a wrap-up code at the end of an interaction before moving on to another interaction.
10. Click **Create**.

Creating an Agent Group

Agent groups form specialized units that receive and place calls. A group is a destination of the service entity in the Connect Contact Center Solution. Calls delivered to the group are presented to the most appropriate agent according to the specified routing policy.

A service defines how a call is processed. Every incoming call to the call center is assigned to a specific service, such as sales, support, and escalations.

The process of creating an agent group involves:

1. *Adding a Group*
2. *Assigning Agents to the Group*

Adding a Group

Creating a group involves specifying the group's name and media capabilities.

Complete the following steps to add a group:

1. From Connect Contact Center Director, click **Groupings** > **Groups**.
2. Click **New**.
3. In the **General** tab, specify the group's name.
4. In the Capabilities area, select the type of media the group can use.

   Each media type requires a license for use by the group. When an agent logs into a group in which a license is required, the number of available licenses is reduced by one. The total number of licenses you have for each media type can be viewed from the Connect Contact Center Director > **Maintenance** > **License** > **License Keys** > **Current Licenses** tab; however the number of licenses for each media type currently in use is not shown.

   - **Chat** — The group is capable of handling chat calls. Each agent that logs in to this group requires a license for handling chat calls.
   - **Dial Lists** — The group is capable of handling outbound dial list calls. Each agent that logs in to this group requires a license for handling outbound dial list calls.
5. Click **Create**.

Assigning Agents to the Group

Once a new group has been added to the system, you assign agents to the group.

Complete the following steps to assign an agent to the group:

1. From Connect Contact Center Director, click **Groupings** > **Groups**.
2. In the List View panel select the group to which you want to assign agents.
3. In the Details View panel, click the **Agents** tab.
4. To add an agent to the group, select the agent in the **Available** list and then click ›. To add all agents to the group, click ».

   The agent is moved from the **Available** list to the **Selected** list.
5. Click **Save**.

Creating a Service

Once you have added a group and assigned agents to it, you need to create a service to be the group's routing destination.

Services define how incoming calls to Connect Contact Center are processed. Services are analogous to a waiting room where calls are managed until they can be answered or otherwise handled. Every incoming call is assigned to a specific service, with defined announcements, overflow and interflow settings, callback settings, and other business rules.

Complete the following steps to create a service:

1. From Connect Contact Center Director, click **Routing** > **Services**.
2. Click **New**.
3. In the **General** tab, specify a name for the service in the **Name** field.
4. Click the **Announcements** tab. In the **Mandatory Announcement** area, select **Enabled** to turn on the mandatory announcement. Then from the **Script** drop-down menu, select a script to be played when callers enter the service.
5. Click the **Destination** tab. From the **Type** drop-down menu, choose **Group**. Then in the Group drop-down menu, select the group for which the service will be the destination.
6. Click **Create**.

Creating an IRN

IRNs are used as entry points to the routing system. Each IRN can be used to define rules for routing the incoming call to various destinations, including services. These rules can also update the call profile, including the call's priority and defining the skills required by the call.

Complete the following steps to create an IRN:

1. From Connect Contact Center Director, click **Routing** > **IRN**.
2. Click **New**.
3. In the **General** tab, in the **IRN** field specify the entry, such as a dial number, to the IRN used to route voice and chat contacts.

Note

The IRN must match a route point in the Mitel Connect system for all voice contacts.

4. Click **Create**.

Create an IVR Port

The IVR subsystem in Connect Contact Center performs various activities including auto-attendant services, announcements, outbound generation of calls, and interactive operations with the caller. IVR ports are first configured as route points in Connect Director.

Complete the following steps to create an IVR Port:

1. From Connect Contact Center Director, click **IVR Configuration** > **Route Points** > **IVR Ports.**
2. Click **New**.
3. In the **General** tab, enter the digits of a dial number in **Route Point Extension** field.
4. From the **IVR Server** drop-down menu, choose the server to which you want to associate the route point.
5. Click **Create**.
6. Use the Contact Center Diagnostics Console to verify that the new IVR Port appears.

Verifying the Call Center Can Receive Calls

Once you have created the basic components of Connect Contact Center, you need to verify that your call center can receive calls.

To verify that the call center can receive calls, dial the Connect Contact Center extension, matching the route point assigned to the IRN in Creating an IRN section on page 64. You will hear a message from Connect Contact Center. Because no agents are logged in and no call handling has been applied, the call will not reach an agent.

Verifying an Inbound Call Reaches an Agent

Complete the following steps to verify that an inbound call reaches an agent:

1. *Logging in as an Agent*
2. *Calling into the System*

Logging in as an Agent

Complete the following steps to log in as an agent:

1. Launch Interaction Center in a browser.
2. Enter agent login credentials defined by an administrator, and then click **OK**.
3. Log into the group by clicking the **Login into my queues** drop-down, and then select a queue.

Calling into the System

To call into the system from a phone not associated with Connect Contact Center, dial the extension matching the route point assigned to the IRN in Creating an IRN section on page 64. The call will be sent directly to an agent logged in to the queue. The Mitel Interaction Center bar changes from

Available/green to Busy/yellow, and the phone rings.

CHAPTER

6

Upgrading, Maintaining, and Troubleshooting Connect Contact Center

This chapter covers information to consider when upgrading Connect Contact Center. Refer to the following sections for details.

Upgrading Connect Contact Center

Upgrading from a previous version of Connect Contact Center is similar to the installation process. However, there are a few things you need to be aware of:

- You can directly upgrade to Connect Contact Center from MCCC 9.
- Mitel supports software-based licensing and no longer requires hardware keys (dongles). This enhances the reliability of the Connect Contact Center system, since there is no dependency on a hardware component. To complete your upgrade, you must request a license key from Mitel order administration (oadmin@shoretel.com). Refer to Requesting a System License Key on page 72 for details about requesting and implementing a new license.
- If you are using the Connect Contact Center redundant server system, before upgrading change your system to manual failover mode using the Connect Contact Center Director > **Maintenance** > **Redundancy** > **Failover Mode** > **Manual** option. This prevents the primary server from restarting as faulty. Once upgrading is complete, you can change your system back to automatic failover mode using the Connect Contact Center Director > **Maintenance** > **Redundancy** > **Failover Mode** > **Automatic** option.
- If there is no database change, which is typically the case, the upgrade process copies the binaries.
- If there is a database change, the upgrade process will upgrade the configuration database, hwich is a quick process, and the contact center will come up and will be ready to take calls. The historical reporting data written *after* the upgrade is accessible to the reporting tools. The historical database upgrade occurs in the background. Because the historical the data is migrated to a new schema, it is not accessible to historical reporting tools until the migration completes.

Agent and Supervisor Records: Upgrading

Class of Service

Agents must be assigned to a Class of Service (COS) in Connect Contact Center. If agents are not already assigned to a COS in MCCC prior to upgrading to Connect Contact Center, they will be assigned to the default COS, which has all COS features enabled by default. The default COS is the first COS record in the list, and the list is ordered alphabetically.

Supervisor records in Connect Contact Center contain a user name, which is different from MCCC 9. You must manually enter the user name for each supervisor in Connect Contact Center. This user name must exactly match the Client username defined for the supervisor user record in the Connect PBX.

Supervisor COS is a new feature, and upon upgrade, every supervisor is assigned to the Standard COS. You must configure the COS features you want the supervisors to have.

Supervisors and Agents

If you have an agent record that has an agent name that matches a supervisor name, and the two records are not associated, the agent record permissions take precedence. In both the Connect PBX and the Connect Contact Center, the user name is what differentiates the record from other records even if the record names match. For example, if you have two records for which the person's name is Bob Smith, each record must have a unique user name.

The Upgrade Process

The upgrade process is covered step-by-step in the following sections:

1. Upgrading Connect Contact Center Systems that Use Email
2. Backing Up the Connect Contact Center System for Upgrade
3. Upgrading the Connect Contact Center Server
4. Upgrading the Distributed IVR Server (Optional)
5. Upgrading a Redundant System (Optional)
6. Upgrading the Chat Toolkit (Optional)
7. Upgrading Client Applications
8. Updating Your Connect Contact Center Licenses
9. Verifying System Functionality

Upgrading Connect Contact Center Systems that Use Email

Note

This procedure is applicable only if you are upgrading the system from MCCC 9 to Mitel MiVoice Connect Contact Center and using the ACD email functionality in MCCC 9. This procedure is not applicable if the system is already on Connect Contact Center and you are performing a maintenance build upgrade.

Because Connect Contact Center includes a change to email configuration, there are additional considerations to make if you are upgrading to Connect Contact Center and use the email feature:

- Ensure your mail server supports IMAP for incoming email account(s), and ensure that you have two additional email accounts available: one for replies and one to act as a dead letter account. If necessary, contact your system administrator for assistance with this procedure.
- Disable any new email downloads to your pre-Connect Contact Center server by disabling all email accounts. You disable email accounts by removing the information in the **Username** and **Password** fields in the **Email** > **Email Accounts** > **Incoming** tab in Connect Contact Center Director.

- Check the **Diagnostic** > **Email** > **Email Accounts** window in the Diagnostics Console to make sure all downloaded emails are routed to agents before your proceed.
- Follow the instructions in Upgrading the Connect Contact Center Server on page 70 to upgrade your Connect Contact Center server.
- Reconfigure email accounts in the **Email** > **Email Accounts** > **Incoming** tab in Connect Contact Center Director.
- Use the **System Parameters** > **Chat and Email** > **Email** > **General** tab in Connect Contact Center Director to configure two email accounts: one for replies and one to act as a dead letter account.
- Reconfigure agent email addresses in the **Agents** > **Agents** > **General** tab in Connect Contact Center Director.

Backing Up the Connect Contact Center System for Upgrade

Backing up the Connect Contact Center system during upgrading is important to provide a failback configuration in case of failure during the upgrade process. Without a current backup, a failed upgrade requires that you rebuild the Connect Contact Center system from scratch. Refer to Backing Up and Restoring Connect Contact Center on page 73 for information.

Upgrading the Connect Contact Center Server

Once you have backed up your Connect Contact Center system, you upgrade the Connect Contact Center Server.

Tip

If you are using the Connect Contact Center redundant server system, stop and disable the Connect Contact Center service on the secondary server, and then delete the MCCC_db_master.sql file from the \Contact Center Server\DBProvider\ folder on the primary server. Following this step makes the upgrading process more efficient.

Complete the following steps to upgrade the Connect Contact Center Server:

1. Ensure no additional users are logged into the server.
2. Download the Connect Contact Center Solution installation files, navigate to the Connect Contact Center Server folder, and click the `setup.exe` file.
3. Follow the instructions in Installing the Connect Contact Center Server on page 25.

Upgrading the Distributed IVR Server (Optional)

If you are using distributed IVR servers to scale the system to more agents, you need to also upgrade these servers.

To upgrade a distributed IVR server, complete the following steps on the IVR station machine:

1. Download the Connect Contact Center Solution installation files, navigate to the Connect Contact Center Server folder, and click the `setup.exe` file.
2. Follow the instructions in Installing Distributed IVR Servers (Optional) on page 42.

Upgrading the CCIR System (Optional)

Note

This procedure is applicable only if you are upgrading from MCCC 9 to Mitel MiVoice Connect Contact Center and were using CCIR in MCCC 9.

If you are using a stand alone CCIR system, complete the following steps to upgrade it:

1. If you have a redundant CCIR system, stop the CC Service on the secondary CCIR system.
2. On the primary system, download the Connect Contact Center Solution installation files, navigate to the Connect Contact Center Server folder, and click the setup.exe file.
3. Follow the installer navigation to complete the installation.
4. When the Diagnostic Console shows the primary CCIR system in a connect state, repeat steps 2 and 3 above to upgrade the secondary CCIR system.

Upgrading a Redundant System (Optional)

In a redundant system, you must upgrade the primary and the secondary server.

Complete the following steps to upgrade the servers:

1. Stop and disable the Connect Contact Center service on the secondary server.
2. Upgrade the primary server software, as explained in Upgrading the Connect Contact Center Server on page 70.
3. Start the primary server if it still needs starting at the end of installation.
4. Upgrade the secondary server software, following the same process you used to upgrade the primary server.
5. Start the secondary server if it still needs starting at the end of installation, and set the Connect Contact Center service back to Automatic.

   After initialization, the secondary server automatically rejoins the system.

Upgrading the Chat Toolkit (Optional)

If you are using the Connect Contact Center chat feature, you should upgrade the chat toolkit. Refer to the *Installing and Implementing Connect Contact Center Chat* guide for information.

Upgrading Client Applications

To upgrade MCCC client applications to Connect Contact Center, Install Connect Contact Center supervisor applications on the system that the supervisor will be using.

Updating Your Connect Contact Center Licenses

Only software license keys are required to operate the Connect Contact Center system. There are two types of software license keys: the system key and feature keys. The system key is a node-locked license tied to your specific Connect Contact Center server. The feature keys enable you to purchase and use specific Connect Contact Center features, including redundancy.

Requesting a System License Key

After upgrading to Connect Contact Center, the first time you launch Connect Contact Center Director the Add New License(s) page is displayed.

Complete the following steps to request a system license key:

1. Make sure your server dongle is still installed on your Connect Contact Center Server.

   The dongle is encoded with information on the specific Connect Contact Center licenses and features you have previously purchased. As part of the upgrade process, the dongle is read to ensure that you have the same licenses and features when you upgrade.

2. From Connect Contact Center Director, click **Maintenance** > **License** > **Request License**.

3. In the **Request System Key** tab, fill in the requested information in the appropriate fields.

   Fields with a title in bold are required.

   The **Contact Email Address** is the email address to which the new license keys are to be sent.

   By default, the fields in the **System Values** area are automatically filled in with information from your Connect Contact Center Server. You should only change this information if you want a license for a server other than the one to which you are currently connected. If you have changed this information, and instead want the default values, click **Restore Defaults**.

Note

If the **BIOS Serial Number** field is blank, either because the server does not have a BIOS serial number or it cannot be read, enter **NOBIOS** in the field.

4. Click **Save**, and then click **Request**.

   The information you entered is displayed, along with details on your currently licensed features.

5. To request your system key now, click **Request Online**.

   Your request for a system key and information on the features you previously purchased are automatically sent to Mitel. The new system key and feature keys are sent to the email address you specified in the **Contact Email Address** field within 3 business days.

6. You can view and print the license request information by clicking **View Request Content**. Your request, and information on the features you previously purchased, are displayed.
7. If you want to request your new system key at a later, more convenient time, click **Save Request to File**. Use the resulting dialog box to save the license information as a `.slr` file.

   When you are ready to request the system key, send the `.slr` file to licensekeyrequest@shoretel.com. The new system key and feature keys will be sent to the email address you specified in the **Contact Email Address** field within 3 business days.
8. Once you have received your license keys, from Connect Contact Center Director click the **Maintenance** > **License** > **License Keys** > **Add New License(s)** tab. Copy the license information from the email and paste it in the **New License(s)** field.
9. Since the feature keys you received are for features already licensed, select **Overwrite Existing Feature Keys**. Your existing feature licenses are overwritten with the new licenses, ensuring that there are no duplicate licenses.
10. Click **Save**.

    The new license keys take effect immediately. You do not need to restart or reboot Connect Contact Center.
11. You can now uninstall the dongle from your Connect Contact Center Server.

Viewing Licensing Information

Information on your Connect Contact Center licenses can be viewed from the Connect Contact Center Director > **Maintenance** > **License** > **License Keys** > **Current Licenses** tab.

Verifying System Functionality

Once you have backed up and upgraded your Connect Contact Center system, you need to verify the system is functioning properly. To do so, run a battery of tests covering all call scenarios.

Backing Up and Restoring Connect Contact Center

Backing up your Connect Contact Center system is an important part of the upgrade process and server maintenance. Regular backups ensure that in the event of a server or application failure, the downtime and data loss experienced by your call center is kept to a minimum.

The Connect Contact Center database can be backed up either automatically or manually. You should use an automatic backup application to back up the other critical components.

The location and handling of your backups should follow your organization's business continuity policies for mission critical systems. It is recommended that you keep a copy off-site to ensure availability of all database backups.

Tip

Refer to the *Backing Up the Connect Contact Center Database*, and *Restoring Connect Contact Center Components* sections of the *Connect Contact Center Administrator Guide* for information about backing up and restoring components of your Connect Contact Center system.

Migrating Enterprise Contact Center from VMware to Microsoft Hyper-V

This section describes how to migrate your existing MCCC from VMware to Microsoft Hyper-V environment.

Backing up MCCC on VMware Infrastructure

1. Log in to Windows DVS, and install the MCCC.
2. Log in to MCCC by using the following default credentials:
   - Username: **ea**
   - Password: **e1996**
3. Add the license information to the License window.
4. Go to the path **\Contact Center Server\DBProvider\ directory**.
5. In the command prompt, run the command **unload_master_db.bat**.
   This creates a database dump file MCCC_db_master.sql with the current log file, and the position information in the same folder.
6. Store the backup file MCCC_db_master.sql on a temporary storage device such as a shared drive, PC or a USB drive.

Restoring MCCC on Hyper-V

1. Log in to the newly installed Windows DVS on Hyper-V, and restore Windows DVS .
2. Install the MCCC.
3. Log in to MCCC director by using the following default credentials:
   - Username: **ea**
   - Password: **e1996**
4. Add the license information to the License window.
5. Stop the Mitel Contact Center service.

6. Go to the path **\Contact Center Server\DBProvider\ directory**.
7. Copy the file MCCC_db_master.sql, which you have stored, from the temporary storage location to**\Contact Center Server\DBProvider\ directory**.
8. In the command prompt, run the command load_master_db.bat. This will load the database backup file.

   After the restore procedure is complete, start the Mitel Contact Center service.

Note

After the migration, the Windows DVS MAC address changes; therefore, you must delete the existing license key, and then request for a new Contact Center license key with a new Windows DVS MAC address. You have 45 days to install the license key.

Troubleshooting Connect Contact Center

This section provides information on problems or errors you may encounter when installing, upgrading, and maintaining Connect Contact Center.

Windows Error Reporting (WER) Support

WER support is now available for the Connect Contact Center Server. WER is a set of Windows technologies that capture software crash and hang data in order to analyze, fix and respond to these problems. Descriptions of problems on your server are sent to Microsoft; Microsoft then sends back either the most current solution or uses the information to start working on a solution.

WER is enabled by default.

System is in Lockdown Mode

Scenario: The Connect Contact Center system is in lockdown mode. In lockdown mode Connect Contact Center Director only displays the License entities. You are unable to log into any other Connect Contact Center supervisor applications or run reports. However, call routing and agent activities are maintained.

Resolution:

- If you have upgraded to a new version of Connect Contact Center, you have not requested and/or entered a new system license key during the 45-day grace period.
- If you are installing a new Connect Contact Center system, you have not updated the system key you initially received with a node-locked system key, as explained in the Requesting and Entering a Node-Locked System Key on page 39.
- If your Connect Contact Center system was previously working, your Connect Contact Center server information has changed (MAC Address, System Volume Serial Number, or BIOS Serial Number). Refer to Requesting and Entering a Node-Locked System Key on page 39 for details.

Error 1720

Error 1720: There is a problem with this Windows Installer Package. A script required for this install to complete could not be run. Contact your support personnel or package vendor.

Scenario: Windows Server 2008 is attempting to install Connect Contact Center. The error appears during the Connect Contact Center installation process, when the installer is creating the database schema.

Resolution: In the Windows Control Panel, turn on the Windows firewall. You are prompted to start the firewall service, click Yes. Then turn off the Windows firewall.