A MITEL
PRODUCT
GUIDE

MiVoice Connect

ST14.2 to MiVoice Connect Migration Guide

Document Version 1.0

July 2022

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Change Log 1

The following table lists the changes made to this document starting with the version published on August 20, 2018. (Changes were not tracked before that version.)

Table 1: Change Log

Document Publishing Date	Changes

July 05, 2022	• Updated the SQL version from 5.7.29 to version 5.7.37 Community Edition in the Install MySQL 5.7 (64 bit) on the Secondary Server on page 36 section.
	• Changed instances of MiVoice Connect version from 19.2 to 19.3 in the following sections:
	  • Important Considerations on page 7
	  • Weeks Before the Upgrade on page 9
	  • CDR Offline Migration on page 34
	  • Install MySQL 5.7 (64 bit) on the Secondary Server on page 36
	• Added a new section Upgrading MiVoice Connect to 19.3 on page 47, which provides information about how to upgrade MiVoice Connect systems running lower than 19.1 SP2 to version 19.3.

May 25, 2021	Made the following updates to step 3 in the section Weeks Before the Upgrade on page 9: • Added the information that UC Server 75 while still supported with MiVoice Connect, reached End of Sale on 15 May, 2020. • Added the information that UC 25 is supported by MiVoice Connect but UC Server 20 is no longer supported by MiVoice Connect. • Added a note that unlike the UC Server 20, the UC Server 25 can be used as an HQ server for small business environments (that have 50 or fewer users).Customers using either of these servers are still advised to migrate to UC Server 30 or to virtualize their SBE deployment instead.

Document Publishing Date	Changes
April 09, 2021	Added a new step in the Weeks Before the Upgrade on page 9 section to inform users that 6900-Series phone might fail after an upgrade to MiVoice Connect version 19.2 because security certificates cannot be successfully verified in some existing circumstances. The 6900-Series phones will successfully register only if the certificate being used is verified, for which the server Common Name (CN) or Subject Alternative Name (SAN) value must match the value in the DHCP scope for Option 156.

November 06, 2020	• Updated the SQL version from 5.6 to version 5.7 in the following sections:
	  • Weeks Before the Upgrade on page 9
	  • CDR Offline Migration on page 34
	  • Install MySQL 5.7 (64 bit) on the Secondary Server on page 36
	• Updated the TLS version from 1.0 to 1.2 in Weeks Before the Upgrade on page 9
	• Updated step 4 in the Weeks Before the Upgrade on page 9 to inform the user to upgrade all systems to the latest version of 14.2 GA30 (19.50.1000.0) prior to the upgrade to MiVoice Connect.
	• Added a note in Important Considerations on page 7 to inform the user that they cannot migrate a 14.2 GA 30 system directly to 19.2 and that it is recommended that they migrate the system to 19.1 SP2 and then upgrade it to 19.2.

Document Publishing Date	Changes

September 07, 2020	• Added a note in the Important Considerations on page 7 section on downloading of Mitel's Windows PowerShell script utility to verify the prerequisites, validate certificates, check system load balancing, and for functions useful for migration preparation and system administration.
	• Added a note in the Important Considerations on page 7 section recommending a review of customer specifics by T3 for large systems (having more than 2000 users) after the document is reviewed and understood.
	• Updated the OneView links to direct the user to the accurate location in the following sections:
	  • Weeks Before the Upgrade on page 9
	  • Upgrade the Appliance Software on page 17
	  • Download the 400-Series Phone Firmware on page 23
	  • Mitel for Salesforce on page 46
	  • Prepare for the Migration on page 49
	  • Before You Upgrade on page 62
	  • Install the Connect for Mobile Clients on page 68

February 07, 2020	• Added a note in Important Considerations on page 7 to capture that the default and custom plan length for both Site Dialing Rules and Trunk Dialing Rule should be less than 2000 characters. • Added a note under step 4 in Weeks Before the Upgrade on page 9 to reflect that all systems be upgraded to the latest version of 14.2 GA30 (19.50.1000.0) prior to the upgrade to MiVoice Connect. • Added a note under step 1 > sub step 4 in Upgrade the Appliance Software on page 17 to indicate that if an SG switch fails to upgrade or is unresponsive, before you proceed to contact customer support, you must see the ***Full Recovery of SG-50v or SG-90v Switches*** KB article for recovery procedure. • Added a new step in Weeks Before the Upgrade on page 9 to reflect that the MiVoice Connect system that you want to migrate has an FQDN address must not contain the "_" character. If the"_" character exists, you must change it before you start the migration process.

Document Publishing Date	Changes
September 30, 2019	• Added a note under step 14 in the Weeks Before the Upgrade on page 9 to reflect the steps to follow if you encounter the **MSVCP140.dll file not installed** error message. • Added a note at the beginning of the Weeks Before the Upgrade on page 9 to reflect that the users must ensure that the FQDN address does not contain the“_” character. This is an invalid character and if included the upgrade process fails. • Added step 4 in the Weeks Before the Upgrade on page 9 to capture that the users must ensure that all 14.2 systems are upgraded to the latest 14.2 version GA30 (19.50.1000.0). • Added step 25 in the Weeks Before the Upgrade on page 9 to reflect that the users must remove any shared drives or folders from the HQ or DVS Servers. • Added a note in the Disable AD Integration Before Upgrade on page 24 to capture that the users must ensure that no AD Group Policy Objects are applied to the HQ Server. It is recommended to remove the server from the AD Domain during migration, to ensure that there is no GPO interference. • Added a note in the One Day Before the Upgrade on page 14 to reflect that the users must remove all 14.2 Communicator Clients from the workstations before they begin the upgrade. if it exists, that will cause problems and lead to service crashes on Connect Servers. • Added a new Connect Client Download on page 45 section and provided the users with the link to download the Connect client.
July 15, 2019	• Added a note under step 13 in the Weeks Before the Upgrade to capture that you must clear the yellow and red phones from the system before you begin the migration. • Added a note under step 6 in the Disable Distributed Database Before Upgrade on page 25 to reflect that when disabling DDB (that is, removal of the local database from a DVS), the DVS server must automatically reboot (restart) to successfully deactivate the feature.

Document Publishing Date	Changes
February 5, 2019	• Revised the information about licensing in Weeks Before the Upgradeand Licensesbecause the process for ordering licenses has changed, and there is no longer a requirement to order SKU 30159. • Added a new step in Prepare for the Upgradeto reflect that if your 14.2 installation is running the Brightmetrics agent for Brightmetrics reports you must stop and disable the Brightmetrics service before performing the upgrade. • Added a new step in After the HQ, DVS, and Appliance Upgradesto capture that if you use the Brightmetrics agent for Brightmetrics reports you must start the service and enable automatic startup for the service.
November 30, 1018	In Upgrade the Headquarters Server Software, added a note about a database error that can occur during the Headquarters server upgrade. The note describes the error and the actions to take if you receive the error message.
November 1, 2018	• Added a note after step 7 in Weeks Before the Upgradeto advise customers who rely on the Mitel Workgroup Monitor application to delay migration until the application is supported in MiVoice Connect. • Revised step 11 in Weeks Before the Upgradeto add a build number and release name for the specific release that ended support for the ShoreGear full-width voice switches. • Added step 24 to Weeks Before the Upgradeto reflect the requirement that TLS 1.0 be enabled on Windows servers. • Updated Rebuild Certificates to Use SHA256to reduce the length of time after migration to wait before rebuilding the certificates.
October 12, 2018	Added a new section: Network Security Port Scans Not Recommended.
September 27, 2018	In Weeks Before the Upgrade, added step 21 about checking the value of the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \ Shoreline Teleworks\Telephony Management Server\ Settings>SwitchDebug**
September 6, 2018	Clarified the step in Weeks Before the Upgradeabout the requirement that ST14.2 and MiVoice Connect use the same installation drive (for example, C:\ or D:\). Added a pointer in this step to a new section about how to change the file system drive of an ST14.2 installation. See Change the File System Drive.
August 28, 2018	Enhanced the information in Licenses

Document Publishing Date	Changes
August 20, 2018	• Added a note about an error message related to the Compatibility Checker to Weeks Before the Upgrade • Added minor clarifications to Back up the ST14.2 System

Migrating the PBX 2

This chapter contains the following sections:

The following sections detail considerations and steps you must make before and during the process of migrating your ST14.2 system to MiVoice Connect.

Important Considerations

This migration process must be performed in lock step for the PBX and Enterprise Contact Center and/or Mobility. After upgrading ST14.2 and the client, you must upgrade the Contact Center and Mobility systems and the related client applications, such as Contact Center Supervisor applications and Connect for Mobile clients, within the same maintenance window.

Note:
You cannot migrate a 14.2 GA 30 system directly to 19.3 or a later release. All the servers and switches must be fully migrated to 19.1 SP2 before the system is upgraded to 19.3 or a later release. The exception is phones, for which upgrading to 19.1 SP2 is optional until the full 19.3 build is installed.

Before migrating, ensure that you access the latest version of this document:

https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform/all-releases/en/st142-to-mivoice-connect-migration-guide

Power User Tools: Download Mitel's Windows PowerShell script utility, "TacTools", to help verify server prerequisites, validate certificates, check system load balancing, and other useful functions for migration preparation and system administration. TacTools is available as a free download from the partner knowledgebase at the following location:

- For Partners: https://mitelcommunity.force.com/partner/s/article/TAC-Tools-Powershell-Scripts
- For Customers: https://mitelcommunity.force.com/customer/s/article/TAC-Tools-Powershell-Scripts

Disclaimer:

The TacTools script was written and provided by TAC. It is provided on a “best effort” basis and is not guaranteed to function properly in your environment. TAC will not troubleshoot the script in a customer’s environment. Many modules are written to be “read only” to minimize any potential impact on the customer’s server. Running any modules that will make any changes to your server will prompt you for confirmation. It is recommended that if you run a module that can make changes to your server, then you must run the script as part of a maintenance window, and must accept any potential service impact caused by the changes made to your server.

You should be aware of some key differences between ST14.2 and MiVoice Connect. These differences are described in Migration Considerations. Read this section before beginning the migration preparation or upgrade steps.

In addition, the following knowledgebase article on the Mitel Support site provides an overview of the feature differences for ST14.2 and MiVoice Connect. You must be logged into MiAccess to access this article:

- For Partners: https://mitelcommunity.force.com/partner/s/article/Feature-Comparison-for-ST-14-2-and-Mitel-Connect-ONSITE
- For Customers: https://mitelcommunity.force.com/cutomer/s/article/Feature-Comparison-for-ST-14-2-and-Mitel-Connect-ONSITE

Note that the default and custom plan combined length for Site Dialing Rules and Trunk Dialing Rules should not exceed 2000 characters.

For Digital Wink Trunks, the number of digits from CO might need to be changed according to the country dial plan. For more information, see the ***Inbound Tab*** section in the ***MiVoice Connect System Administration Guide***.

Note:
After you have reviewed and understood this document, Mitel recommends a review of the customer specifics by T3 for large systems (more than 2000 users). In this situation, you must open a case with the following details:

```
Subject: Request for pre-Migration T3 review

# servers:

# and type of switches:

# locations:

Network topology details:
```

```
# and type of phones:

ECC/Mobility (y/n and # agents/users):

Pro Svcs and/or 3rd party apps and where installed:

Size of CDR and archive CDR:

Run TACtools and share results for:
```

- RTC scores:
- Server prereqs:

2.1 PBX Migration Steps

To prepare your system for the upgrade to MiVoice Connect, you must complete some steps during the weeks before the migration, the day before the migration, and the day of the migration.

2.1.1 Weeks Before the Upgrade

1. Review the Build Notes for the MiVoice Connect system that you are planning to migrate to.
2. Evaluate and schedule your organization's training needs as follows:
   - End-user training is necessary due to the changes in operation and differences between the Communicator Client and the new Connect Client. Users need to understand these differences and be instructed on the personal data they must back up or change to avoid its loss during the migration to MiVoice Connect.
   - Administrator training is recommended because of major differences in the administrative interfaces in MiVoice Connect.
3. Upgrade any 32-bit OS servers to 64-bit OS servers.

   See Build Notes for supported OSs, and the ***Migrating from 32-bit Windows Server to 64-bit Windows Server*** section of the ***Planning and Installation Guide*** for details of this procedure.

   Also see the ***UC Server 75, UC Server 25, and UC Server 20 (Legacy Servers)*** section in the ***Planning and Installation Guide***. UC Server 75, while still supported by MiVoice Connect, reached End of Sale effective 15 May, 2020. UC Server 20 is an outdated server and is not supported by MiVoice Connect. However, UC Server 25 is supported by MiVoice Connect and earlier versions of ST14.2.

Note:
Unlike the UC Server 20, the UC Server 25 can be used as an HQ server for small business environments (50 or fewer users). It can also be used as a Distributed Voice Server (DVS) on MiVoice Connect. However, customers using either of these servers are still advised to migrate to UC Server 30 or to virtualize their SBE deployment instead.

4. Ensure that all 14.2 systems are upgraded to the latest 14.2 version GA30 (19.50.1000.0). You must upgrade all systems to the latest version of 14.2 GA30 (19.50.1000.0) before you upgrade to MiVoice Connect. This is to facilitate the database cleanup that occurs during the upgrade to MiVoice Connect. If you are moving the systems directly to MiVoice Connect, only the servers (HQ/DVS) and appliances (SA100/400) require an upgrade to 14.2 GA30.
5. Ensure that your ST14.2 installation is running on the same platform (hardware and OS) that will be used for your MiVoice Connect installation:
   - If your ST14.2 system is not running on the same platform that will be used for MiVoice Connect, you must move your ST14.2 system to the appropriate platform prior to starting the migration process. The common platform for both ST14.2 and MiVoice Connect is Windows Server 2012 R2 64-bit.
   - Subsequent OS upgrades, such as to Windows Server 2016, can only be completed after the migration to Connect is complete.
6. Ensure that your ST14.2 installation uses the same drive (for example, C:\ or D:\) that will be used for your MiVoice Connect installation. (If you want to install MiVoice Connect on a different drive, you must move your ST14.2 installation to the new drive before the migration to MiVoice Connect. For information about how to change the file system drive of your ST14.2 installation, see Change the File System Drive.)
7. To obtain the necessary licenses for the MiVoice Connect system, send an email to license.support@mitel.com with the information described in Licenses.
8. Confirm that any Mitel Professional Services applications are updated to versions that are compatible with MiVoice Connect.

Note:

Customers with a heavy business dependency on the Mitel Workgroup Monitor application should delay the migration to MiVoice Connect until further notice. The application is not supported with the currently recommended MiVoice Connect build. Mitel Engineering is working diligently to correct this limitation.

9. Confirm that any third-party applications are updated to versions that are compatible with MiVoice Connect.
10. Ensure that all ST14.2 systems you are upgrading have current licenses that are in compliance.
11. Ensure that your SG half-width switches are running boot RAM version 1.1.3.29 or higher. For details, see Ensure that Voice Switches Have Latest Boot ROM Version.
12. The legacy ShoreGear full-width voice switches (ShoreGear 120/24, ShoreGear 40/8, ShoreGear 60/12, ShoreGear T1, and ShoreGear E1) will not be supported in MiVoice Connect as of the July 9, 2018 release (build 21.88.3731.0, R1804). If you have these voice switches, do not include them in the migration process.
13. Download the latest Connect software from the following site and distribute it to all servers that will be upgraded:

    - For Partners: https://mitelcommunity.force.com/partner/s/article/Connect-Software
    - For Customers: https://mitelcommunity.force.com/customer/s/article/Connect-Software

14. Download the latest firmware for the 400-Series and 6900-Series IP phones to all 400-Series phones, but do not upgrade the phones. For details, see Download the 400-Series Phone Firmware on page 23.

> **Note**:
>
> Clear the yellow and red phones from the system before you begin the migration. This ensures that no unused/old phones are migrated.

15. Run the Compatibility Checker from the MiVoice Connect installation package on the Headquarters server, and correct any resulting database issues. Continue to run the Compatibility Checker after each database correction until it returns no errors. (You can access the Compatibility Checker in the Tools folder in the MiVoice Connect installation location.)

Note:

If the **MSVCP140.dll file not installed** error message appears when you attempt to run the Microsoft Visual C++ Redistributable 2015 (x86 and x64) or if crash dumps are generated for KadotaUtil.exe and QuickInstall.exe, do the following:

- Ignore the crash dumps generated for KadotaUtil.exe and QuickInstall.exe.
- Install Microsoft Visual C++ Redistributable 2015 (x86 and x64) and rerun the compatibility checker. For more information, see the following KB Article:
  - For Partners: https://mitelcommunity.force.com/partner/s/article/Error-1723-while-installing-Connect-PBX-Software
  - For Customers: https://mitelcommunity.force.com/customer/s/article/Error-1723-while-installing-Connect-PBX-Software

16. Run the Compatibility Checker on the DVSs and correct any errors.
17. If you have active directory (AD) integration configured, create a non-AD administrator account in Director.
18. Confirm that the Headquarters server has available drive space. As a best practice, Mitel recommends that 40 GB of storage be available, but ensure that at least 30 GB is available.
19. Delete abandoned unplugged phones from Director.
20. Download Microsoft Updates as per the Connect Build notes. (In many cases these updates can be downloaded but not installed.)
21. Confirm that all the current installation ST14.x software is available on all ST14.2 servers, which you can use in the very unlikely scenario of a failed migration that requires reinstalling the ST14.2 software.
22. In the registry on the Headquarters server, locate the following registry key:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Shoreline Teleworks \Telephony Management Server\Settings->SwitchDebug

    Look for an **ether_mtu_size 1300** entry where 1300 is the MTU size that Mitel uses for all Ethernet traffic. Due to a known defect, the DRS service (which is always running, even if DRS is not enabled) will not function if the MTU size specified in the registry is anything but 1400. (The correction for this defect will be available in a future release of MiVoice Connect.) If this value is anything other than 1400, determine why the MTU size was adjusted and either correct that limitation (and remove the registry entry) or delay the migration until the defect fix is available. The most common reason for adjusting the MTU size is for communication links over VPN services that do not support the Mitel default MTU size of 1400. Absence of the registry entry indicates the system is utilizing the default size of 1400.

23. Because of the schema change between MySQL 5.6 and MySQL 5.7, you must remove any customizations you defined for your CDR and restore the CDR to the default configuration before the migration. (After migration, you can re-implement the customizations.)

> **Note**:
> Before you upgrade your system from WB.2 to MiVoice Connect, it is mandatory that you disable the Distributed Database feature. After the upgrade process is complete, if required, you can manually re-enable the Distributed Database feature.

24. If your ST14.2 installation uses virtual appliances, be aware that VMware administrative access must be available on the day of migration to enable the SCSI controller change that is necessary for virtual appliances.
25. Remove any shared drives or folders from the HQ or DVS Servers. If a user has a server file locked from another computer, it can disrupt the migration and be difficult to diagnose.
26. Mitel 400-Series IP phones and other solution components in MiVoice Connect require TLS 1.2 for connectivity. TLS 1.2 is enabled by default on Windows servers, but administrators can disable it. Perform the following steps to confirm that TLS 1.2 is enabled on all ST14.2 servers:

    a. Navigate to **Control Panel** > **Internet Options**, and select the **Advanced** tab.
    b. Scroll to the bottom of the **Settings** and confirm that **Use TLS 1.2** is selected.
27. Ensure that the MiVoice Connect system that you want to migrate has an FQDN address that does not contain the "_" character. If the "_" character exists, you must change it before you start the migration process.
28. The improved security implementation in MiVoice Connect version 19.3 might cause 6900-Series phone registration failures after upgrading because security certificates cannot be successfully verified in some existing circumstances. The networks use DHCP Option 156 to point the phones to the proper configuration server. The 6900-Series phones will successfully register only if the certificate being used is verified, for which the server Common Name (CN) or Subject Alternative Name (SAN) value must match the value in the DHCP scope for Option 156. Thus, if the DHCP scope contains the server's FQDN while the certificate contains the server's IP address, the certificate will not be verified and the phone registration fails. To prevent this, it is recommended that you use the configuration server's FQDN in both the DHCP Option 156 and in the certificate's **Subject Alternative Name** field. If the certificate value matches the value in the DHCP scope, the certificate will be successfully verified and the 6900-Series phones will be registered. Therefore, before you upgrade MiVoice Connect to version 19.3, you must ensure that the server identified in the certificate and in the DHCP scope must match. Additionally, the 6900-Series phones must know the current time for validating the expiration dates of the HTTPS certificates. Configuring DHCP Option

42 with the IP address of a reachable NTP server will allow the phones to update the date and time before trying to register securely.

2.1.2 One Day Before the Upgrade

Note:

- Before you begin the upgrade, remove all 14.2 Communicator Clients from the workstations. If 14.2 Communicator Clients are present after the migration, these clients will attempt to connect to services that no longer exist. This will cause problems and lead to service crashes on Connect Servers.
- In large deployments users are grouped by departments. Before you begin the upgrade, you must temporarily remove the Configuration switch settings. This will prevent IP phones from jumping to other SG switches after the SG switches reboot.

1. Download any recorded conferences from your service appliances. For details, see Recordings.
2. In ST14.2 Director, use the Batch Update utility to change all **Personal** licenses to **Professional** licenses.
3. If your ST14.2 installation uses virtual appliances, confirm that an administrator with VMware administrative access will be available on the day of migration to implement the SCSI controller change that is necessary for virtual appliances.

2.1.3 Day of the Upgrade

For more information about installing MiVoice Connect, see the ***MiVoice Connect Planning and Installation Guide***. For details about configuring MiVoice Connect using Connect Director, see the ***MiVoice Connect System Administration Guide***.

Note:

Before you begin the upgrade, you must delete any full-width switches. If not, you will experience service interruptions until the TDI Media Driver is reinstalled.

2.1.3.1 Prepare for the Upgrade

1. Back up the ST14.2 system. The configuration database, CDR database, Web Bridge database, and other data must be copied to a safe location prior to migration. For backup instructions and a complete list of data to back up, see Back up the ST14.2 System.
2. If you use Enterprise Contact Center, back up the ECC application. For details, see Back Up the Enterprise Contact Center Components.
3. Install any recommended Microsoft Server updates on the HQ server, as indicated in the Build Notes.
4. In ST14.2 Director, disable IP phone failover.
5. If applicable, disable Active Directory (AD) integration in ST14.2. For details, see Disable Active Directory (AD) Integration Before Upgrade.
6. If applicable, disable Distributed Database on the DVS servers in ST14.2. (Note: SG90V and SG50V voice switches must first be pointed to the HQ database. Also be aware that DVSs will reboot when Distributed Database is disabled.) For details, see Disable Distributed Database Before Upgrade.
7. Disable Anti-Virus software and Windows Firewall on the HQ server.
8. If the ST14.2 Headquarters server is running the Brightmetrics agent for Brightmetrics reports, open **Windows Administrative Tools** and then open **Services**. Right click the **Brightmetrics service** and select **Properties**. Stop the service and change the **Startup type** to **Disabled**.

2.1.3.2 Upgrade the Headquarters Server Software

1. Run **setup.exe** as Administrator on the HQ server.

   The duration of the upgrade depends on the server performance. The upgrade process could take in excess of one hour. Do not attempt to stop the upgrade without first contacting Mitel Support.

Note:

If you see the following error message during the Headquarters server upgrade process, review the referenced log file and search for an entry that includes “RelCOSTAcceptWhisperPagingDN”:

Fatal Error - A database exception has occurred. Please review the Database log in the Shoreline Data\Logs folder.

This error message refers to corruption in the ST14.2 database for a Class of Service setting for Whisper Paging in which the **Whisper Paging** option is set to

Accept Only from with an extension field that either contains an invalid extension number or is blank, as shown here:

To address this issue, do one of the following:

- Contact Mitel TAC to have the database manually corrected.
- In ST14.2 Director, do the following:

  a. For each Class of Service, change the **Whisper Paging: Accept:** setting to **None**.
  b. Save the changes.
  c. Attempt the Headquarters server upgrade again.

A future release of the Compatibility Checker will flag this database issue prior to migration.

2. After the upgrade completes, when prompted reboot the HQ server.
3. Launch Connect Director, and do the following:

   a. Enter your credentials to log in. When prompted, reset your password to complete the log-in process.
   b. Verify that the following pages load correctly:

      - **Administration** > **Users** > **Users**
      - **Administration** > **Appliances/Servers** > **Platform Equipment**
      - **System** > **Administrative Permissions** > **Administrators**
      - **Reporting** > **Report Options**
      - **Maintenance** > **Status and Maintenance** > **System**
      - **Maintenance** > **Status and Maintenance** > **Appliances**

   c. Make a name change to a user, save it, and confirm that the change was applied.
   d. Revert the change you made in the previous step.
   e. Re-enable Active directory integration in Connect Director by navigating to **Administration** > **System** > **Additional Parameters** and selecting the**Enable AD integration** option.
   f. Log into Connect Director as an AD user.

2.1.3.3 Upgrade the Distributed Voice Server (DVS) Software

Perform the following steps for every DVS in your system:

1. Install any recommended Microsoft Server updates, as indicated in the Build Notes, on the DVSs.
2. Disable Anti-Virus software and Windows Firewall on the DVSs.
3. Run **setup.exe** as Administrator on the DVSs.
4. When prompted, reboot the DVSs.
5. Verify that the installation process completed with no errors.
6. Verify server status in Connect Director by navigating to **Maintenance** > **Status and Maintenance** > **Servers**
7. In Connect Director, re-enable Distributed Database for DVSs. For details, see Enable Distributed Database After Upgrade.

> **Note**:
>
> The DVSs will reboot.

2.1.3.4 Upgrade the Appliance Software

Perform the following steps for every appliance in your system:

1. In Connect Director, navigate to **Maintenance** > **Status and Maintenance** > **Appliances**, and do the following:

   a. Sort by “Site”.
   b. Select 10-12 switches to upgrade. (The number of switches upgraded simultaneously will vary based on WAN/LAN connectivity.)
   c. From the **Command** drop-down lists at the top of the page, select **Reboot and Reset** and **Reboot Appliances**.
   d. The upgrade for virtual appliances requires a type change for the SCSI Controller in VMware for CentOS. For details, see Upgrade Virtual Appliances from ST14.2 Wind River Linux to CentOS.

Note:
If an SG switch fails to upgrade or is unresponsive, before you proceed to contact customer support, see the following KB Article that will help you with recovery:

- For Partners: https://mitelcommunity.force.com/partner/s/article/Full-Recovery-of-SG-50v-or-SG-90v
- For Customers: https://mitelcommunity.force.com/customer/s/article/Full-Recovery-of-SG-50v-or-SG-90v

e. Reconfigure the database reference for each Voicemail switch. For details, see Enable Distributed Database After Upgrade.

2. When all switches are online, in Connect Director navigate to **Maintenance** > **Status and Maintenance** > **IP Phones** and confirm that 400-Series IP phones are upgrading to the latest MiVoice Connect firmware for 400-Series IP phones.

Note:
In MiVoice Connect, by default, 400-Series IP phones are upgraded automatically.

3. Upgrade any MGCP phones by using the commands on the same IP Phones status page.
4. When all IP phones are online, do the following:

a. In Connect Director, navigate to **Administration** > **Telephones** > **Options** and select the **Enable IP phone failover** option.
b. Test basic calling functionality for internal calls, external calls, workgroups, voicemail, and so on.

2.1.3.5 Upgrade the Connect Client Software

Push or manually install the Connect client software. You can obtain the Connect client installation package from the Mitel Support site or from Connect Director by navigating to **System** > **Downloads**. Users will be prompted to reset their passwords. For more information about installing the Connect client, see the ***Connect Client User Guide***.

2.1.3.6 Regenerate Certificates

Regenerate self-signed certificates on any service appliances (SA-100/SA-400). For details, see Regenerate Self-Signed Certificates for Service Appliances.

2.1.3.7 After the HQ, DVS, and Appliance Upgrades

1. Re-enable Anti-Virus software and Windows Firewall on servers where necessary.
2. If you archive the CDR, follow the relevant procedures for your installation that are described in Back up and Restore the Archive CDR.
3. Implement any MySQL customizations you defined for your CDR that you removed before the migration.
4. If you had an extension configured for recording auto attendant prompts and workgroup names, this setting is not carried over during the migration. You will need to reconfigure this setting in Connect Director after the upgrade is complete. See Reconfigure Extensions for Recording Auto Attendant Prompts and Workgroup Names for details.
5. If you have Enterprise Contact Center, proceed with the ECC upgrade during the same maintenance window. For details on the ECC migration process, see Prepare for the Migration on page 49.
6. If you have Mobility, proceed with the Mobility upgrade during the same maintenance window. For details on the Mobility migration process, see Before You Upgrade on page 62
7. If you use Mitel for Salesforce, you need to perform some steps after the migration. For more information, see Mitel for Salesforce .
8. If the Brightmetrics agent was disabled prior to migration, open **Windows Administrative Tools** and then open **Services**. Right click the **Brightmetrics service** and select **Properties**. Start the service and change the **Startup type** to **Automatic**.

2.1.4 Post Migration

Rebuild Certificates to Use SHA256

The unified communications system automatically generates a Headquarters root certificate authority (CA) certificate when the system is first installed. This root CA signs various certificates used by voice switches, servers, and phones. The Root CA certificate is preserved when you migrate from ST14.2 to MiVoice Connect. The root CA certificate in ST14.2 uses the SHA1 algorithm, which is being phased out for security reasons. Therefore, after the migration process you must rebuild the Headquarters root CA certificate to use the SHA256 algorithm, using the procedure in Rebuild the Headquarters Server Root Certificate as SHA256.

Important: Prior to making the certificate change to SHA256, verify all call functionality in the newly migrated Mitel MiVoice Connect system. For larger systems (1,000+ users), best practices dictate three to four hours of stability (all green status in Diagnostics and Monitoring in Connect Director, and no major events recorded) to confirm correct system connectivity before rebuilding the certificates to use SHA256. Depending on time constraints, the certificate change to SHA256 might require scheduling another maintenance window days or weeks after the migration to complete the procedure.

2.2 Additional Details for Migration Sub-procedures

The following procedures provide details for some of the high-level steps included in PBX Migration Steps and Day of the Upgrade.

2.2.1 Change the File System Drive

If you want to install MiVoice Connect on a drive that is different from the drive where your ST14.2 system is installed (for example, change from C:\ to D:\), before the migration you must change the drive of the ST14.2 system to the new target drive using the procedures described in the following two subsections. The process involves moving all of the relevant files from the original (source) file system to the new target file system.

2.2.1.1 Steps to Perform on the ST14.2 Original (Source) File System

1. In Director, disable the Active Directory setting (if enabled) for the administrator's account.

2. Back up the databases using the following commands and copy the files to another location.

   - CDR

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\backupCDR.bat
     ```

   - Configuration database

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\backupConfig.bat
     ```

   - WebBridge database

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\backupWebBridge.bat
     ```

   - Monitoring database

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\backupMonitoring.bat
     ```

3. Stop and disable all ST14.2 services by running the following batch file:

   ```
   <Install drive>\Program Files (x86)\Shoreline Communications
   \ShoreWare Server\Scripts\hq_shoretel-stop-svcs.bat
   ```

4. Use the following steps to confirm that all ST14.2 services have stopped:

   a. Go to the **Windows Run** menu
   b. Type **services.msc**
   c. Review all of the services to ensure that they show “Manual” and that the services are stopped.

5. Copy the Shoreline Data folder (excluding the \Database folder) to a safe location and label the version and build in the folder in which it is located. It is highly recommended that you copy off the server to a safe location. Mitel recommends that you back up these files to a storage device separate from the server that you intend to upgrade.
6. Uninstall Shoreware from the server.
7. Reboot.
8. Delete the content from the Shoreline Data folder and all ShoreTel folders from Program Files (x86).
9. Delete the following registry key structures if they are still present after the uninstall process:

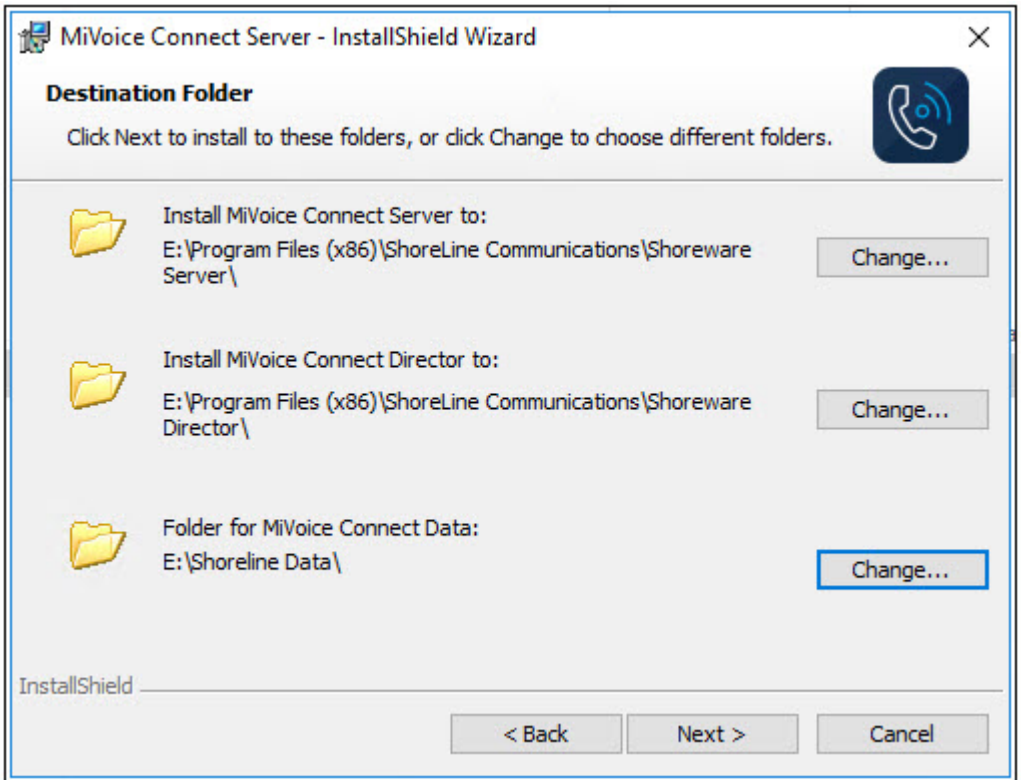
   - **HKLM\SOFTWARE\Wow6432\MySQL AB\MySQL Server**
   - **HKLM\SOFTWARE\Wow6432\Shoreline Teleworks**

10. Reboot.

2.2.1.2 Steps to Perform on the New (Target) File System

1. Copy the Shoreline data folder that you copied earlier to the new drive. If you renamed the folder during the backup process, be sure to rename it back to Shoreline Data on the new install drive.
2. Install on top of the old Shoreline Data folder the exact same version of the ST14.2 server software that was installed before. (When installing the ST14.2 server on Windows Server, you must launch **Setup.exe** using **Run as Administrator**.

Figure 1: Installing ST14.2 Server Windows Server



3. Reboot (as part of install process).
4. Copy keystore folder from the backup onto the Shoreline Data folder.

5. Restore the database backups made previously, as follows:

   - To import the CDR database dump:

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\
     MySQL\MySQL Server\Examples\RestoreCDR.bat
     ```

   - To import the Config database dump:

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\
     MySQL\MySQL Server\Examples\RestoreConfig.bat
     ```

   - To import the WebBridge database dump:

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\RestoreWebBridge.bat
     ```

   - To import the Monitoring database dump:

     ```
     <install dir>\Shoreline Communications\ShoreWare Server\MySQL
     \MySQL Server\Examples\RestoreMonitoring.bat
     ```

6. Reboot.
7. Log in to Director

2.2.2 Download the 400-Series Phone Firmware

To prepare the 400-Series phones for the migration process, you should download the latest phone firmware to the phones' second partition so that it is ready to install after the migration.

1. Download the setup.exe file for the phone firmware to the Headquarters server and to any Windows DVSs. For details about where to find the **setup.exe** file, see the following KB Article:

   - For Partners: https://mitelcommunity.force.com/partner/s/article/Connect-Software
   - For Customers: https://mitelcommunity.force.com/customer/s/article/Connect-Software

2. On the Headquarters server, run the **setup.exe** file.

   The firmware build is added to the `<ftproot>/phones/<build number>`directory.

3. On the Windows DVSs, run the **setup.exe** file.
4. Launch Director.
5. Click **Maintenance** > **Status and Maintenance** > **IP Phones**. The **IP Phones** page is displayed.
6. Select the check box for each phone to which you want to download the firmware.
7. In the Command drop-down menu, select **Download**.
8. Click **Apply**.

9. In the **Confirmation** dialog box, click **Advanced**.
10. For each type of phone selected, in the **Version** drop-down list select the firmware version that corresponds to the firmware you downloaded.
11. Click **OK**.

2.2.3 Back up the ST14.2 System

1. Back up the configuration database on the HQ server using the following command as an administrator:

   ```
   <drive>:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\backupConfig.bat
   ```
2. Back up the CDR database on the HQ server using the following command:

   ```
   <drive>:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\backupCDR.bat
   ```
3. Back up the Web Bridge database (for SA-100/SA-400) on the HQ server using the following command:

   ```
   <drive>:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\backupWebBridge.ba
   ```
4. Back up the registry on the HQ server.
5. Back up the ftproot folder on the HQ server.
6. Back up the following folders from the Shoreline Data folder on HQ:
7. Back up the following folders from the Shoreline Data folder on each DVS:

   - Vms
   - UserData
   - Keystore

2.2.4 Disable AD Integration Before Upgrade

You must disable Active Directory (AD) integration in ST14.2 prior to upgrading to MiVoice Connect. Complete the following steps to disable AD integration:

Note:

Ensure that no AD Group Policy Objects are applied to the HQ Server, as described in the ***MiVoice Connect Planning and Installation Guide***. It is recommended to remove the server from the AD Domain during migration, to ensure that there is no GPO interference.

1. Launch ST14.2 Director.
2. Navigate to **Administration** > **System Parameters** > **Other**.
3. Deselect **Enable AD Integration**
4. Click **Save**.

2.2.5 Disable Distributed Database Before Upgrade

Disable distributed database (DDB) before the upgrade to prevent sync errors that might prevent the upgrade from completing.

1. Launch ST14.2 Director.
2. Navigate to **Administration** > **Platform hardware** > **Voice Switches Service Appliances** > **Primary**.
3. For each Voicemail switch (SG90V, SG50V), for future reference note the DVS referenced for the distributed database, and then change the **Use database on server** option to **Headquarters Server**.
4. Navigate to **Administration** > **Application Servers** > **HQ/DVS**.
5. Select the appropriate DVS, and in the edit page, deselect **Enable Local Database**.
6. Click **Save**.

Note:

- When disabling DDB (that is, removal of the local database from a DVS), the DVS server must automatically reboot (restart) to successfully deactivate the feature. You must confirm this before the migration.
- To confirm this, open the registry editor on the DVS that had the DDB disabled and go to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Shoreline Teleworks`.
- Confirm that **LocalDBServerAddress** is the HQ IP address and **LocalDBServerID** is set to **1**.
- If the these settings are still set for **DDB**, reboot the HQ server, then reboot the DVS server, and check the DVS registry editor settings again.

2.2.6 Enable Distributed Database After Upgrade

Complete the following steps to enable distributed database in Connect Director:

1. Launch Connect Director.
2. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**.
3. Select the appropriate DVS or Voicemail switch, and on the **General** tab, select **Enable Local Database**
4. Click **Save**.

2.2.7 Ensure that Voice Switches Have Latest Boot ROM Version

The Boot ROM for the SG half-width switches should be 1.1.3.29 or higher. If the boot ROM version is lower than 1.1.3.29, you should upgrade the boot ROM prior to upgrading the ST14.2 system to MiVoice Connect.

You can verify the boot ROM version in ST14.2 by navigating to the **Maintenance** > **Status** > **Switches** > page in the Diagnostics and Monitoring system and checking the value in the **Boot ROM Version** field on the **Status** tab.

To update the Boot ROM, do the following:

1. Connect to the SG half-width switch by using Telnet or Secure Shell (SSH).
2. Go to Shell by typing **gotoshell**

3. Enter the `uboot_update` on the CLI.

   The switch will be restarted to update the Root ROM.
4. Verify the Boot ROM version by navigating to the **Maintenance** > **Status** > **Switches** > page in the Diagnostics and Monitoring system and checking the value in the **Boot ROM Version** field on the **Status** tab.

2.2.8 Upgrade Virtual Appliances from ST14.2 Wind River Linux to CentOS

When you upgrade existing virtual appliances (vPhone, vTrunk, and vCollab) from ST14.2 to MiVoice Connect, they are migrated from Wind River Linux to CentOS. In addition to supporting VMware, CentOS provides the capability to support Microsoft Hyper-V.

Use the following procedure to update all virtual appliances during the migration process. This procedure, which involves changing the SCSI Controller type, applies only to virtual appliances, not to physical appliances.

1. Upgrade the appliance by using Connect Director. Refer to the *Voice Switches* chapter in the *MiVoice Connect Maintenance Guide* for information about the upgrade procedure.

> **Note**:
>
> Selecting the check box to apply an upgrade to all appliances in the **Maintenance** > **Status** and **Maintenance** > **Appliances** page selects only the appliances on that page. If you want to upgrade more appliances than those shown on a page, you must manually select additional appliances on the subsequent pages.

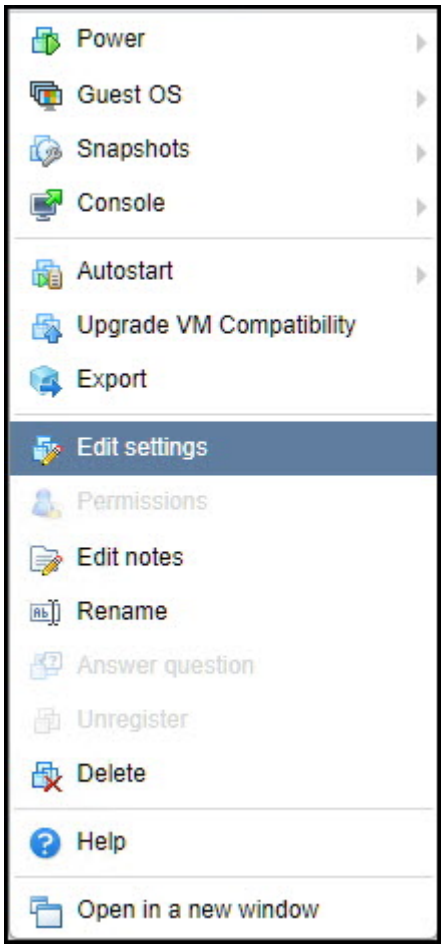
2. Log in to the **vSphere** console with administrative access.
3. As the virtual appliances are upgraded, watch for the following messages, which are generated because CentOS does not support the BusLogic Parallel type for the SCSI controller. This is the point at which you must change the SCSI controller type to VMware Paravirtual if it is BusLogic Parallel.

   Warning: dracut-initqueue timeout – starting timeout scripts

   Entering emergency mode. Exit the shell to continue

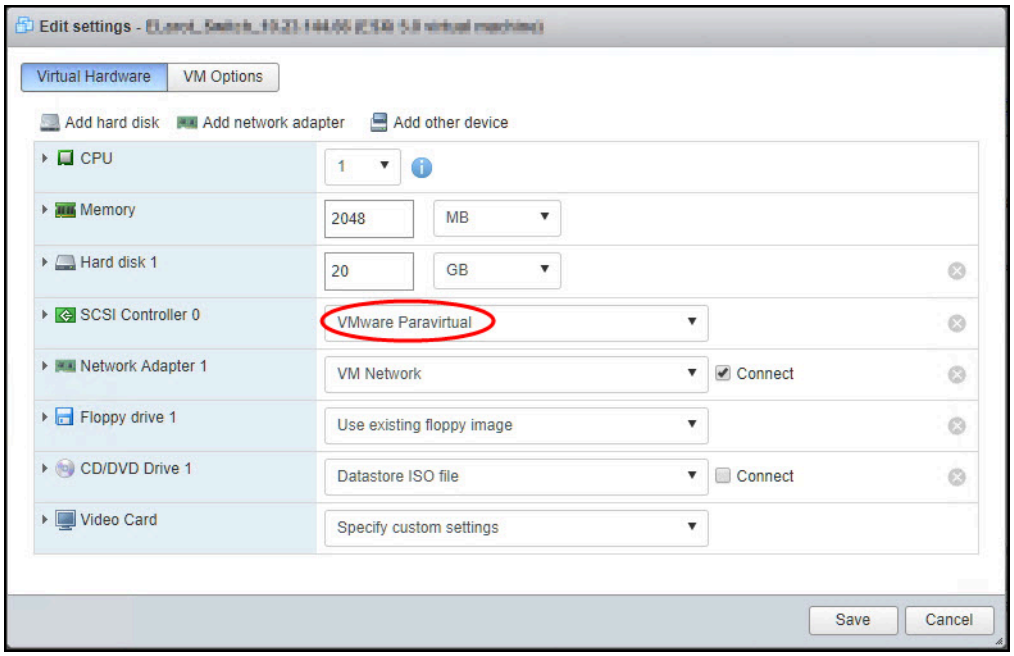
4. Shut down the Virtual Machine, and click **Edit settings**.

Figure 2: Edit Settings Option



5. On the **Virtual Hardware** tab of the **Edit Settings** window, change the **SCSI Controller 0 type** field to **VMware Paravirtual**, and click **Save**.

Figure 3: Virtual Hardware Tab



The Appliance is upgraded to CentOS and restarted.

6. In Connect Director, verify that the status indicator for the selected appliance is green.
7. To verify that each appliance has been upgraded to CentOS, do the following:

   a. Enter the root/ShoreTel or admin/ShoreTel credentials in the Command Line Interface (CLI).
   b. Type **cat /etc/centos-release** and press **Enter**. The CentOS version detail appears.
   c. Type **stcli**.

2.2.9 Regenerate Self-Signed Certificates for Service Appliances

If you are using a global URL and self-signed certificates on your Service Appliance, you must re-generate self-signed certificates for your appliance after upgrading to MiVoice Connect to successfully create conferences.

Note:

All service appliances and IP phones must be in sync with Time server before regenerating the self-signed certificates.

Complete the following steps to regenerate self-signed certificates for a service appliance:

1. Complete the following steps to disable HTTPS for the service appliance:
   a. Launch Connect Director with administrative privileges.
   b. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**
   c. On the list pane, click the service appliance for which you want to configure HTTPS, and then click the **HTTPS** tab
   d. Select the service appliance in the Disable HTTPS on the following service appliance dropdown list, and click **Go**.
   e. Before proceeding, wait five minutes for the service appliance to stabilize.
2. Use PuTTY to access the service appliance, and navigate to the `/cf/certs` directory on the device.
3. Delete the following files:
   - ucb_server.key
   - ucb_ca_cert.crt
   - ucb_ssl_cert.crt
4. Complete the following steps to enable HTTPS for your service appliance:
   a. Launch Connect Director with administrative privileges.
   b. Navigate to **Administration** > **Appliances/Servers** > **Platform Equipment**
   c. On the list pane, click the service appliance for which you want to configure HTTPS, and then click the **HTTPS** tab.
   d. Select the service appliance in the Enable HTTPS on the following service appliance dropdown list, and click **Go**.
5. Use PuTTY to access the service appliance, and ensure that files you deleted in step 3 are recreated in the `/cf/certs` directory on the device.

2.2.10 Rebuild the Headquarters Server Root Certificate as SHA256

The following procedure applies to the 1804-PREM Release (build 21.88.3731.0) or higher:

1. On the **Maintenance** > **Status and Maintenance** > **Appliances** page in Connect Director check to ensure that the status is green for all voice switches that host 400-Series IP phones. (Green status indicates that a switch is connected to the TMS service, which is required for this procedure.) Any 400-Series IP phones that are not “In service” will not receive the updated certificate and will require the MUTE CLEAR# process to clear each phone’s configuration and bring the phones back into service.
2. On the **Administration** > **System** > **Additional Parameters** page in Connect Director, verify that the **Require secure client access (https)** option is not selected. If this option is selected, uncheck the option and click **Save**. Log out from Connect Director and close the browser.

> **Note**:
>
> Disabling HTTPS in Connect Director is required in case any issues occur after regenerating the certificate.

3. On the HQ server and each DVS, run the **Microsoft Management Console (mmc.exe)** and load the Certificates snap-in. Remove the following certificates:
   - HQ
     - Remove all <HQ_FQDN_or_IP> certificates from the Personal Store.
     - Remove all ShoreTel UC Certificate Authority certificates from the Trusted Root Certification Authorities Store.
   - DVS
     - Remove all <DVS_FQDN_or_IP> certificates from the Personal Store.
4. On the HQ server, make a backup copy of `<drive>:\Shoreline Data \keystore`outside of the `<drive>:\Shoreline Data` folder. Also, back up the configuration database on the HQ server using the following command:

   ```
   <drive>:\Program Files (x86)\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\BackupConfig.bat
   ```

Note:

- You must be certain of your `Keystore` folder backup. Normally, you should never delete the `Keystore` folder. This SHA256 rebuild is a special, one-time case. In general, deleting the `Keystore` folder or any of the keys causes far more problems than it solves.
- If needed, rename the current database backup file to avoid it being overwritten if BackupConfig.bat was run previously.

5. On the HQ server, in <drive>:\Shoreline Data\keystore\certs, delete the following certificate files:
   - hq_ca.crt
   - hq.crt
   - server.crt
   - <HQ_FQDN_and/or_IP>.crt
6. On the HQ server, in the Windows Services control panel, restart the **ShoreTel-WebFrameworkSvc** service. This causes the Headquarters root CA certificate to be regenerated, which then causes all the other certificates signed by this root CA to be rebuilt. Wait 15 minutes for the HQ server to stabilize.
7. In the **Administration** > **Appliances/Servers** > **Platform Equipment** page in Connect Director, select each DVS (one at a time), click the Certificate tab in the lower pane, click **DELETE CURRENT CERTIFICATE**, confirm delete, and then click **Save**. Perform this step for every DVS. This rebuilds the DVS certificate and remotely restarts the **ShoreTel-WebFrameworkSvc** service on the DVS. It might take up to two minutes for the regenerated certificate to show up in Connect Director after reloading the Certificate tab.
8. On the HQ and each DVS server, run the Microsoft Management Console (mmc.exe) and load the Certificates snap-in. In the Personal Store, double-click the <HQ/DVS_FQDN_or_IP> certificate to open it. At the bottom of the General tab for the HQ server and each DVS, if there is the message “You have a private key that corresponds to this certificate” with a small key icon next to, proceed to the next step. Otherwise, see Troubleshooting.
9. Confirm that all phones are working.

2.2.10.1 Troubleshooting

If you do not see the message **You have a private key that corresponds to this certificate** at the bottom of the General tab for the <HQ/DVS_FQDN_or_IP> certificate, run the following steps first for the HQ server and then for each DVS.

1. In the **Administration** > **Appliances/Servers** > **Platform Equipment** page in Connect Director, select the HQ or DVS server, click the **Certificate** tab in the lower pane, click **DELETE CURRENT CERTIFICATE**, confirm delete, and then click **Save**.
2. Wait two minutes for the HQ or DVS certificate to regenerate.
3. On the HQ or DVS server, run Microsoft Management Console (mmc.exe) and load the Certificates snap-in. In the Personal Store, double-click on the <HQ/DVS_FQDN_or_IP> certificate to open it. At the bottom of the General tab, you should now see the message **You have a private key that corresponds to this certificate** with a small key icon next to it.

2.2.11 Back up and Restore the Archive CDR

If you archive your CDR, follow the procedures that pertain to your installation as described in this section.

2.2.11.1 Backing up the Archive CDR on a Secondary Server

Note:
Throughout this section, information shown inside <> is variable depending on information you define for your system.

Complete the following steps to back up an archive CDR that is stored on a secondary server:

1. Back up the archive CDR server using one of the following methods:

   a. Navigate to `<installation location>\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples`, and make a copy of `BackupCDR.bat`. Modify the file name of the copied batch file. Modify the contents of the file to change shorewarecdrdump to the appropriate archive database name, and modify the name of the resulting SQL file.

   Run the new batch file from the command line to create `<drive designation>\<archivedatabase>.sql`.

   b. Run a backup using SQLyog: Select the remotecdrarchive DB, right-click the database name, and select **Backup/Export** > **Backup DB** as SQL dump.

2.2.11.2 CDR Offline Migration

Because of the schema change between MySQL 5.6 and MySQL 5.7, the Connect installer prompts you to take a back up of your CDR before you begin the upgrade. To streamline the process of upgrading the CDR with these schema changes, the Connect installer includes an offline CDR migration that runs in the background after the Connect installation is complete. You can view the progress in the Connect Director Diagnostics and Monitoring page once the installation has completed.

Once the installation of Connect is complete and while the CDR offline migration process is running, you will be able to report against the new CDR data that is accumulated while the PBX is running, but you will not be able to report against the old CDR data.

You can view the status of the CDR Offline migration in the **Maintenance** > **Status and Maintenance** > **Servers** page of Connect Director when you select the HQ server.

Note:

- If the CDR offline migration fails, the system cannot be upgraded or patched. This migration must be completed successfully and temporary migration services (cDR UPG and CDR migration-UPG) must be deleted prior to applying any patches or hot fixes. These services are deleted automatically upon the successful completion of the CDR offline migration. If the migration does not complete successfully, contact Mitel for assistance.
- If the CDR offline migration process continues beyond midnight, no data will be archived for the day in which the migration process began. In this scenario, archive will resume at midnight the day after the migration began.

2.2.11.3 Restore Archive Databases

In general, to restore archive databases, stop all services except for MySQL, and then use MySQL command lines and batch files to restore archive databases. After restoring archive databases, restart services and check the status in the servers page of Connect Diagnostics and Monitoring.

Refer to the sections below for specific information about restoring archive databases locally and remotely.

Restore the Local CDR Archive

1. After the Connect installation is complete, you must verify that the `Archive.ini` file is located at `<installation location>\Shoreline Communications \ShoreWare Server`.
2. Open a command prompt, and enter the following commands to create an archive database:

   ```
   cd “<installation location>\Shoreline Communications\ShoreWare Server” MakeCDRArchive.exe -d <DBName>
   ```

   `<DBName>` is the name of the archive database to be created, such as `CDRArchive`.

   If the archive process is successful, this step creates a new CDR database, which you can view in SQLYog.
3. Complete one of the following steps to restore the archive data dump created in Disable Active Directory (AD) Integration Before Upgrade:

   - Open a command prompt on the Headquarters server, and enter the following command to restore the database:

     ```
     cd “<installation location>\Shoreline Communications \ShoreWare Server\MySQL\MySQL Server\Examples” restoreCDR -r
     ```
   - Use SQLyog to restore the database:

     Select the archive database, right-click, and select Restore from SQL Dump. Select the file created in Disable Active Directory (AD) Integration Before Upgrade, and then click on **Execute**.
4. To upgrade the restored version of the database to the new schema, open a command prompt, and enter the following commands to create an archive database:

   ```
   cd “<installation location>\Shoreline Communications\ShoreWare Server” MakeCDRArchive.exe -d <DBName>
   ```
5. When you have completed these steps to restore the archive database, run any reports you have configured for the Headquarters and archive servers, and check the reports for accuracy.

CDR Archive on the Secondary Server

1. After the Connect installation is complete and the Headquarters server restarts, uninstall MySQL 5.7 and ODBC drivers on the secondary archive server using the Control Panel.
2. Check `<installation location>\MySQL\MySQL Server 5.7\data\` to verify that there are no MySQL folders remaining after the uninstall is complete. If there are folders or files in this location, delete them.

3. On the secondary server, create a directory called `<drive location>\Shoreline Communications\ShoreWare Server\MySQLCDR\MySQL Server`.

Install MySQL 5.7 (64 bit) on the Secondary Server

1. Start the installation process, selecting the products you want to install, and then click **Next**.

   If you are doing a clean install, click Advanced Features, and then complete the Path Conflicts screen:

   a. Specify the path you created in step 3 above as the location for installing MySQL 5.7.37 Community Edition.
   b. Click **Next**.
2. Click **Execute** in the Installation screen.
3. Complete the **Type and Networking** screen:

   a. Select **Development Machine** in Config Type, and enter **4309** in **Port Number**. TCP/IP and Open Firewall port for network access are enabled by default.
   b. Click **Next**
4. Complete the **Accounts and Roles** screen:

   a. Enter **shorewaredba** as the MySQL Root Password and Repeat Password in the **Accounts and Roles** screen.
   b. Click **Next**
5. Complete the **Windows Service** screen:

   a. Select **Configure MySQL Server**as a Windows Service.
   b. Enter **MYSQL** in Windows Service Name.
   c. Select **Start the MySQL Server**at System Startup.
   d. Click **Next**.
6. Click **Execute** in the **Complete the Apply Server Configuration** screen.
7. Click **Finish**.

Install and Verify the ODBC 5.3.4 (32-bit) Driver

You must install this 32-bit ODBC driver because the MakeCDRArchive is a 32-bit application.

Note:

The following are the pre-requisites to install this 32-bit application on 64-bit operating systems:

- For any supported version of Windows Server, the Microsoft C++ 2010 x86 runtime libraries must be installed. If they are not, visit the Microsoft web site to download the Microsoft Visual C++ 2010 Redistributable Package (x86).

Refer to the Software Build notice for information about supported versions of Window Server.

Complete the following steps to install the 32-bit ODBC driver:

1. Launch the MySQL Community installer that you installed in Install MySQL 5.7 (64 bit) on the Secondary Server on page 36.
2. Click **Add**, expand the MySQL Connectors item, and then select **Connector/ODBC 5.3.4 X86**.
3. Click the right arrow to move Connector/ODBC 5.3.4 X86 to the Products/Features To Be Installed section.
4. Click **Next**, and then click **Execute** to complete the installation.

When installation is complete, view the ODBC driver version in the registry editor to verify that the 5.3.4 X86 version is installed.

Configure the Archive on the Secondary Server

The secondary archive server is a 64-bit Windows server. You specify the IP address and other information for this server in the **Reports** > **Options** page in Connect Director on the Headquarters server.

1. Copy the contents of `<installation location>\Shoreline Communications \ShoreWare Server\MySQLCDR\MySQL Server` to a safe location.
2. Copy the `<installation location>\Shoreline Communications \ShoreWare Server\MySQLCR\MySQL Server\Data[ib_logfile*]` to a safe location, such as `<drive designation\MySQL_backup`.
3. Click **Start** > **Administrative Tools** > **Services** > **MySQL**.
4. Select **Stop the service**, and then verify that the MySQL service status is **blank**.

5. Verify that the following two files have their parameters set the same way:

   - File on the Headquarters server: `<installation location>\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples\archive_MySQL_my.ini`
   - File on the secondary server file: `<installation location>\Shoreline Communications\ShoreWare Server\MySQLCDR\MySQL Server\my.ini.`

   Note:

   In the event the my.ini file is not on the secondary server, copy it over from the Headquarters server and then proceed with the remainder of these steps.

   - Parameter settings should have the following values:
     - mysql

       default-character-set = utf8
     - mysqld

       character-set-server = utf8
     - tmp_table_size = 30M
     - key_buffer_size = 2M
     - read_buffer_size = 2M
     - read_rnd_buffer_size = 2M
     - sort_buffer_size = 2M
     - innodb_additional_mem_pool_size = 2M
     - innodb_flush_log_at_trx_commit = 0
     - innodb_log_buffer_size = 5M
     - innodb_buffer_pool_size = 150M
     - innodb_log_file_size = 24M
     - default-storage-engine = INNODB
6. In SQLYog, add a new connection with the following credentials and port setting:
   - User: **root**
   - Password: **shorewaredba**
   - Port: **4309**
7. Delete the `<installation location>\MySQL\MySQL Server 5.7\Dat\ib_logfile*` file where the asterisk represents a wildcard.

8. In the `<installation location>\MySQL\MySQL Server 5.7\my.ini` file, verify that the **innodb_flush_log_at_trx_commit** value is set to **zero** (innodb_flush_log_at_trx_commit=0). If this value is not set to zero, the archiving write operation will be very slow.
9. Click **Start** > **Administrative Tools** > **Services** > **MySQL**.
10. Select **Start the service**, and then verify that the MySQL service comes back up.

Create an Archive CDR on the Secondary Server

Complete the following steps to create a CDR archive on the secondary server:

1. To create a CDR archive database, copy the following files from the Headquarters server, and paste them into `<installation location>\Shoreline Communications\ShoreWare Server` on the secondary server:
   - MakeCDR.dll
   - MakeCDR.sql
   - MakeCDR_sp.sql
   - MakeCDRArchive.exe
2. On the Headquarters server, navigate to the `<installation location>\Shoreline Communications\ShoreWare Server\MySQLCDR\MySQL` Server directory, copy the archive.ini file, and paste the file in the same directory on the secondary server.
3. Edit the `archive.ini` file to have correct MySQL version.
4. Open a command prompt, and enter the following commands to create an archive database:
   - `cd <installation location>\Shoreline Communications\ShoreWare Server`
   - `MakeCDRArchive.exe -d <DBName>`

   `<DBName>` is the name of the archive database to be created, such as “RemoteCDRArchive”.
5. To verify the creation of the database, open SQLYog and using the information in the left panel, explore to verify that the archive file name specified in step 4 is correct. Also, expand the table to ensure that it appears correctly.

6. Complete one of the following steps to restore the archive data dump created on the Headquarters server:

   a. Copy restoreCDR from the Headquarters server to `<installation location>\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples` on the secondary server.

      Modify restoreCDR to change the name of the database to be restored to the name of the archive database, and then change the name of the file to the same as was created in Backing up the Archive CDR on a Secondary Server.

      Open a command prompt on the secondary server, and enter the following command to restore the remote archive database:

      ```
      cd “<installation location>\Shoreline Communications\ShoreWare Server\MySQL\MySQL Server\Examples” restoreCDR -r
      ```

   b. Use SQLyog to restore the database: Select the remote archive database, right-click, and select restore from SQL Dump. Select the file you created in step 1 of the Backing up the Archive CDR on a Secondary Server section, and then and then click **Execute**.

7. To upgrade the restored version of the database to the new schema, open a command prompt, and enter the following commands to create an archive database:

   ```
   cd “<installation location>\Shoreline Communications\ShoreWare Server”

   MakeCDRArchive.exe -d <DBName>
   ```

8. When you have completed these steps to restore the archive database, run any reports you have configured for the Headquarters and archive servers, and check the reports for accuracy.

   Be aware that restoring the archive database may be a lengthy process. You may not have access to reports until the restoration process is complete.

2.2.12 Reconfigure Extensions for Recording

If your system had an extension configured for recording auto attendant prompts and workgroup names, this setting is not carried over during the migration. You will need to reconfigure this settings in Connect Director after the upgrade is complete.

To reconfigure the extension used for recording auto attendant prompts and workgroup names:

1. Launch Connect Director.

2. Do one of the following:

   - Navigate to **Administration** > **Features** > **Auto-Attendant**, and then select the **On-Hours**, **Off-Hours**, **Holiday**, or **Custom tab**.
   - Navigate to **Administration** > **Features** > **Workgroups**, and then select the **General** tab.
3. Under **Recorded prompt** or **Workgroup name**, click **Preferences**. The **User Preferences** dialog box appears.
4. In the **Record using** field, enter the extension to use for recording auto attendant prompts and workgroup names.
5. Click **Save**.

2.3 Migration Considerations

The following sections highlight differences between ST14.2 and MiVoice Connect that you should be aware of.

2.3.1 Licenses

Customers migrating from ST4.2 to MiVoice Connect are entitled to functionality that required the purchase of additional licenses in ST14.2. Historically, the process for acquiring these no-charge licenses required the partner to place a $0 order for part number 30159 and then wait for that order to flow through the system to the Licensing Support team for fulfillment.

The new process, which can be completed in a few days, involves simply sending an email to license.support@mitel.com following the template below:

- Email subject: **Connect Upgrade**
- Email body must include the following information:

  - End Customer ID number
  - End Customer name
  - System name(s) if customer has multiple systems
  - Partner ID number and name
  - Additional email addresses, in addition to the sender who should receive the licensing reply

Note:

A single email can be sent for customers with more than one system.

Upgrade licenses will be generated for all systems specified in the request.

The customer will receive licenses for all UC applications in the MiVoice Connect Essentials license bundle for all Extension & Mailbox, Extension Only and Mailbox Only licenses on active support in their customer asset list.

Depending on the customer asset list, the following additional license keys and entitlements could be included:

- Desktop Client
  - Professional Call Manager
  - Soft Phone
  - Standard Resolution Video
- Mobile Client
  - Mobile Call Manager
  - SIP Device for Mobility
- Advanced Applications
  - Web Dialer
  - App Dialer
- Right to use Connect Telephony for Microsoft and Connect for Chrome (no license key)

To take advantage of any additional MiVoice Connect functionality such as Remote Phone, CRM integration, Work Group and Operator, contact your Mitel representative about which MiVoice Connect license bundle uplift from Essentials best meets your needs.

2.3.2 Service Appliances

Refer to the following sections for important considerations regarding Service Appliances and conferencing.

2.3.3 Recordings

The update to MiVoice Connect includes a change in the conference bridge that does not migrate current recordings, and you must archive any recordings you want to keep.

Prior to migrating from Communicator to Connect client, download the service appliance recordings made with Communicator and save them to the local system. While the downloaded recordings cannot be played in the Connect client, you can use a Flash-enabled Web Browser to play them.

Complete the following steps to preserve previous conference recordings; you must archive them on a per-user basis:

1. Open a browser, navigate to the web conference bridge, and log in.
2. Navigate to the **My Conferences** tab, and click **Recordings**.
3. Select the conference recording you want to download, and then click the appropriate download option.
4. Repeat these steps for each conference recording you want to archive.

2.3.4 Reservationless Conferences

Note:

- The **Allow participants to IM** option is no longer available in MiVoice Connect. Therefore, ensure to set this option to the required setting before migrating. This is true not only for reservationless conferences but for conferences in general.
- When an administrator deletes a conference in Connect Director, the conference might still appear in the Connect client even though it is no longer valid. Users cannot remove the invalid conference from the client. If the user tries to join the web or audio conference, he/she receives an error message indicating that the participant code is not valid.

See the following items for information about how reservationless conferences migrate from Communicator to Connect client:

- Users who have a reservationless conference that was previously configured in Communicator and who are assigned to a service appliance will have a

reservationless conference created during migration, and the settings defined previously will remain valid.

While access codes on a migrated reservationless conference remain valid, the When dialing out to participants parameter in the event screen will always be set to **Must press one to enter audio portion of the meeting** regardless if the conference was previously configured with **Participants are automatically added to the audio portion of the meeting**.

- Users who do not have a reservationless conference previously configured in Communicator but who are assigned to a service appliance will have a reservationless conference created during migration, and the settings defined previously will remain valid.
- Users who do not have a reservationless conference previously configured in Communicator and who are not assigned to a service appliance will not have a reservationless conference created during migration.

2.3.5 Communicator

You must be aware of the following behavior differences between Communicator and the Connect client.

2.3.5.1 IM Considerations

Before upgrading the ST14.2 PBX to MiVoice Connect, in ST14.2 Director configure all Mobility users who will be using Mobility client 9.0 to have their IM configuration changed to a collaboration appliance (SA-100 or SA-400).

2.3.5.2 Favorites

If you have created a Favorites group in Communicator, rename this group before migrating to Connect. Connect client contains a Favorites group at install, and if you have not renamed your Favorites group in Communicator prior to upgrade, you may lose that data.

2.3.5.3 Speed Dial Numbers

Before migrating from Communicator to Connect client, delete all the speed dial numbers you have configured in Communicator.

If you do not delete the speed dial numbers before the migration, these numbers will be stored in Connect database. However, you cannot access these speed dial numbers on the Connect client.

When you receive an incoming call, from a number where the assigned name is changed after migration, the Connect client might still display the old name assigned to the Speed Dial number as stored in the database before migration.

2.3.5.4 Call Routing Rules

You must be aware that personal call routing rules that you defined in Communicator will migrate to the Connect client, but these routing rules might not work as you expect.

2.3.5.5 Connect Client Download

You can download the Connect client from **http://<Server IP>/ShoreWareResources/clientinstall/default.htm**.

2.3.6 Passwords

Beginning with MiVoice Connect, password strength requirements are significantly more strict to help protect your PBX system. Upon first login to the MiVoice Connect Director, the Connect client, the Connect for Mobile client, and the MiVoice Connect Contact Center system, you might be prompted to change your password or get an indication that your password has expired. This is likely due to the existing passwords that migrated over to the new system not meeting strength requirements. Follow the prompts to reset passwords.

Refer to the ***Configuring the Password Policy*** section in the ***MiVoice Connect System Administration Guide*** for information about creating strong passwords.

2.3.7 Network Security Port Scans Not Recommended

Mitel recommends that you not run port scans against Mitel appliances in MiVoice Connect.

Running port scans against Mitel appliances can cause an issue in which phones assigned to the scanned appliances go to a **No Service** state for a short period of time (from a few seconds to a few minutes). If you notice this behavior in phones, you can confirm this issue by using SSH to connect to the phones' assigned appliance and looking for messages such as the following:

```
stelshark / telnet not enabled
```

2.3.8 Enhanced Mobility Extension

While the migration to MiVoice Connect in combination with the migration to the Mobility Router 9.0 does not change user details such as the enhanced mobility extension or the client username, be aware that modifying any other part of the enhanced mobility

user’s record in Connect Director will modify the mobility application number configured for the user. This modification will invalidate the SIP registration for the enhanced mobility user. When the SIP registration is invalidated, the enhanced mobility user will not be able to use the mobility application on his or her device. To work around this issue, the administrator must modify the user’s profile in the Mobility Router to match the changed settings in MiVoice Connect Director.

2.3.9 Mitel for Salesforce

For information about steps to take to update an existing Mitel for Salesforce configuration from ST14.x to MiVoice Connect, see the following KB Article:

- For Partners: https://mitelcommunity.force.com/partner/s/article/Mitel-for-Salesforce-Migrating-from-ST14-to-Connect
- For Customers: https://mitelcommunity.force.com/customer/s/article/Mitel-for-Salesforce-Migrating-from-ST14-to-Connect

Upgrading MiVoice Connect to 19.3 3

MiVoice Connect systems running releases earlier than 19.1 SP2 must be upgraded to 19.1 SP2 before upgrading to 19.3.

For information about upgrading the MiVoice Connect system to version 19.3, see the relevant sections in the MiVoice Connect Planning and Installation Guide:

- ***Upgrading the Server System***
- ***Upgrading MiVoice Connect Server***
- ***Upgrading the DVS Software***

Migrating ECC9 to MiVoice Connect Contact Center

4

This chapter contains the following sections:

The following sections detail considerations and steps to take before, during, and after completing the process of migrating your Enterprise Contact Center 9.0 installation to MiVoice Connect Contact Center.

Introduction

This document provides a high-level process for migration of the Enterprise Contact Center version 9 to Mitel MiVoice Connect Contact Center. It covers the migration of the Contact Center servers and CCIR.

4.1 Important Considerations

- The MiVoice Connect Contact Center requires the PBX to be MiVoice Connect version 21.82.2142.0 or higher. If you are running ST14.x (or lower), upgrade the PBX to MiVoice Connect before upgrading Contact Center.
- Mitel suggests upgrading to MiVoice Connect Contact Center version 507.84.8206.0 or higher.
- Prior to upgrading the Contact Center Server software, ensure that the procedures to back up the Contact Center server(s) and upgrade the Remote Server (DVS) Software have been completed successfully.
- With MiVoice Connect, the Agent Toolbar is removed and the Mitel Interaction Center is a thin client that runs as a web application only. The ability to transfer calls from the Interaction Center is limited to other Contact Center users only. To transfer calls to extensions outside of Contact Center, use the Connect client.
- Beginning with the MiVoice Connect PBX and MiVoice Connect Contact Center, the client username defined in the PBX must exactly match the agent username and supervisor username records defined in MiVoice Connect Contact Center. If you need to make changes to ensure this information matches exactly, Mitel strongly suggests you make changes in MiVoice Connect first: **If you need to make changes in the MiVoice Connect Contact Center to match what's defined in the PBX, you must restart the MiVoice Connect Contact Center service for the change to properly sync with the MiVoice Connect PBX database.**

4.2 Prepare for the Migration

To prepare your Enterprise Contact Center 9 system for the upgrade to MiVoice Connect Contact Center, perform the following steps during the weeks before the migration:

1. Review the Build Notes for the MiVoice Connect Contact Center system that you are planning to migrate to.
2. Determine the training needs and coordinate scheduling for Contact Center agents, supervisors, and administrators. Training is strongly recommended due to the changes in the user interfaces.
3. Upgrade any 32-bit OS servers to 64-bit OS servers. For details, see the following KB Article:
   - For Partners: https://mitelcommunity.force.com/partner/s/article/Moving-Mitel-Contact-Center-to-a-New-Server
   - For Customers: https://mitelcommunity.force.com/customer/s/article/Moving-Mitel-Contact-Center-to-a-New-Server
4. Download the MiVoice Connect Contact Center Software from the Mitel Support site.
5. Determine the location for the MiVoice Connect Contact Center backups.
6. Ensure that Contact Center Server has sufficient available disk space on C:/.

> **Note**:
>
> Mitel recommends 40 GB of available space, but you must have at least 20 GB of available space.

7. Confirm the starter account **ea** is configured as a **System Administrator** and is enabled. For details, see Ensure that the Starter Account Exists.
8. If no other Supervisor Administrator accounts are configured in Contact Center Director, create an additional Supervisor account.

> **Note**:
>
> This step is required to access Supervisor tools

9. The Agent Toolbar is replaced with the Mitel Interaction Center, a thin client that runs as a web application. Prepare to uninstall the Agent Toolbar from the Agent's station after the upgrade is complete.
10. Review Agent Wallboards in use and review options for KPI Boards.
11. If AD Integration is enabled on the PBX, verify that the Agent Email Address is set to the corporate email address in Contact Center Director. For details, see Update Agent Settings (Non-Supervisor).
12. If AD Integration is not enabled on the PBX, document the agent and supervisor's Client ID setting from 14.2 Director. For more information, see Syncing Data Between PBX and Contact Center.
13. If CCIR is installed on your ECC server, uninstall CCIR and install on a separate server.
14. Determine if Brightmetrics is installed and/or required on CCIR.

4.3 Upgrade Enterprise Contact Center to MiVoice Connect Contact Center

Upgrading the ST14.2 Enterprise Contact Center to MiVoice Connect Contact Center involves the following tasks, which are described in more detail in the subsequent sections:

- Back up the Enterprise Contact Center server
- Turn off redundancy, if enabled
- Upgrade the Primary server to Mitel MiVoice Connect Contact Center
- Turn on redundancy, if applicable
- Upgrade CCIR, if applicable
- Upgrade Chat
- Upgrade the IVR
- Update Agent and Supervisor settings
- Update Agent and Supervisor applications

4.3.1 Back Up the Enterprise Contact Center Components

Note:

Ensure that at least 20 GB of space is available on the server before backing up the Enterprise Contact Center components.

1. Back up the Contact Center Server (all data) as follows:

   a. Navigate to **Contact Center Director** > **Maintenance** > **Database Backup**.
   b. Select **All Data**.
   c. When complete, copy the backup to an alternate location.
2. Back up the following Contact Center server folders:

   - `<drive>:\Program Files x86\ShoreTel\Contact Center Server \Agents`
   - `<drive>:\Program Files x86\ShoreTel\Contact Center Server\IVR`
   - `<drive>:\Program Files x86\ShoreTel\Contact Center Server \backup`
3. Back up any “custom” folders that may contain reports, audio files, and so on.

Refer to *Enterprise Contact Center Administrator Guide* for ECC 9.0 for information about backup procedures

4.3.2 Turn Off Redundancy (If Enabled)

1. If a Secondary (redundant) Contact Center server is present, verify that redundancy is set to manual failover by navigating to **Maintenance** > **Redundancy** > **Failover Mode** > **Manual** option.
2. On the **Secondary** (redundant) Contact Center Server, stop and disable the Contact Center service.
3. On the **Primary** Contact Center server, delete the `ecc_db_master.sql` file from the `\ShoreTel\Contact Center Server\DBProvider` folder (if present).

4.3.3 Upgrade MiVoice Connect Software on Primary Contact Center Server

1. Disable the Firewall and the Anti-Virus software on the Primary MiVoice Connect Contact Center server.
2. Run the MiVoice Connect Contact Center Server **setup.exe** as **Administrator**.
3. When prompted, enter the FQDN or IP address of the Primary Contact Center Server.
4. Set the Authentication URL to **https://<IP** or **FQDN of HQ>/shoreauth**.
5. Set Boostrap URL to **https://<IP** or **FQDN of HQ>/shorestart**.
6. When the upgrade is complete, uncheck **Start Contact Center Now**.
7. Manually reboot the Contact Center server.

8. When the server is back online, log into MiVoice Connect Contact Center Director as follows:
   - log in with **ea**, use **http://servername/contactcenterdirector** (which can only be accessed from the MiVoice Connect Contact Center server).
   - To log in with Supervisor accounts, use **http://<servername>:3000/ccd** .
9. Launch the Diagnostics Console to view the status.

> **Note**:
>
> Log in with a supervisor account; **ea** will not work.

10. Launch Activate Window Viewer application (located in the `\ShoreTel\ShoreTel Contact Center Server` folder) to monitor the progress of the observation tables. Historical reports will not work until this process is complete.

> **Note**:
>
> Do not reboot the Contact Center Server until the observation table update is complete, as indicated by the **DbUpgrade:OBSERVATION ended** message. This process can take several hours.

4.3.4 Upgrade MiVoice Connect on the Secondary (Redundant) Server

If your environment contains a redundant Contact Center Server, follow these steps to upgrade the Secondary (redundant) Contact Center Server:

1. Disable the Firewall and the Anti-Virus software on the Secondary MiVoice Connect Contact Center server.
2. Run the MiVoice Connect Contact Center Server **setup.exe** as **Administrator**.
3. When prompted, enter the FQDN or IP address of the Primary Contact Center Server.
4. Set the Authentication URL to **https://<IP** or **FQDN of HQ>/shoreauth**.
5. Set Boostrap URL to **https://<IP** or **FQDN of HQ>/shorestart**.
6. When the upgrade is complete, uncheck **Start Contact Center Now**.
7. Manually reboot the Secondary Contact Center server.

8. On the Primary MiVoice Connect Contact Center server, launch the Diagnostics Console to verify the status of Redundancy.
9. If Redundancy was set to **Manual** prior to the upgrade process, set it back to **Automatic** by navigating to the **Contact Center Director** > **Maintenance** > **Redundancy** > **Failover Mode** > **Automatic** option.
10. On the MiVoice Connect Contact Center Primary Server, navigate to `<MiVoice Connect Contact Center installation location>\nginx\conf`, and copy the following files:

    - `nginx_ecc.template`
    - `readme.txt`
    - `Redundancy.bat`
    - `Redundancy_config.rb`
11. On the MiVoice Connect Headquarters server, navigate to the `<MiVoice Connect installation location>\nginx\conf\more_conf directory`, and paste the files you copied in step 10.
12. Double-click the **Redundancy.bat** file.
13. When the Windows console loads, follow the instructions on the console, and enter the IP addresses of the Headquarters server, Primary Contact Center Server, and Secondary Contact Center Server.
14. Restart the ShoreTel-DirectorProxy service as follows:

    a. In the **Windows Start** menu, click **Control Panel** > **Administrative Tools** > **Services**.
    b. Select the **ShoreTel-DirectorProxy** service, and click **Restart**.

4.3.5 Upgrade CCIR

1. If you have CCIR on a secondary server, stop the CCIR service on the secondary server.
2. Copy the **CCIR** folder from the MiVoice Connect Contact Center Software installation package to the primary CCIR server.
3. Disable Anti-Virus software and Firewall on the primary CCIR server.
4. Run the **setup.exe** as **Administrator** on the primary CCIR server.
5. Follow the prompts to install the software on the primary CCIR server.
6. If prompted, reboot the primary CCIR server.
7. When the CCIR server is **online**, check the CCIR status through the **Diagnostics Console**.
8. Upgrade the secondary CCIR server by following steps 2-7, modifying the instructions for the secondary server.

4.3.6 Upgrade Chat

1. Copy the **Chat Server** folder from the MiVoice Connect Contact Center Software installation package to the Chat server.
2. Disable Anti-Virus software and Firewall on the Chat server.
3. Run the **setup.exe** as **Administrator**.
4. Follow the prompts to install the software.
5. When the Chat upgrade is complete, check the status of Chat in the **Diagnostics Console**.

4.3.7 Upgrade the IVR

1. Copy the **IVR** folder from the MiVoice Connect Contact Center Software installation package to the IVR server.
2. Disable Anti-Virus software and Firewall on the IVR server.
3. Run the **setup.exe** as **Administrator**.
4. Follow the prompts to install the software.
5. If prompted, reboot the IVR server.
6. When the IVR upgrade is complete, check the IVR status in the **Diagnostics Console**.

4.3.8 Update Agent Settings (Non-Supervisor)

1. To determine the required setting for Agent Username in the agent record in Connect Contact Center Director, log in to the MiVoice Connect Director and navigate to Administration > Users > Users.
2. Select the user, and do the following:
   - If AD Integration is enabled, select **Sync from AD** to pull the valid Client Username.
   - If AD Integration is not enabled, use the Client Username configured for the user.
3. Log in to **Connect Contact Center Director** and select the agent record.
4. Update the Agent Username to match the Client Username (from step 2 above).

4.3.9 Update Supervisor Settings

Depending on whether or not the supervisor's Agent Email Address was set to the Client Username before migration, use one of the following procedures to update the supervisor settings.

4.3.9.1 Scenario 1

For **Supervisors who are Agents, are AD enabled, and whose Agent Email Address was set to the Client Username (that is, corporate email address) prior to the migration**:

1. Log in to MiVoice Connect Director:
   a. Verify the Client Username of the Supervisor by navigating to **Administration** > **Users** > **Users**. Select the user and click **Show from AD** or **Sync from AD**.
   b. Turn off AD Integration for the user.
   c. Click **Save**.
   d. Manually set the Client Username to match what the AD Client Username returned in step 1a above.
   e. Click **Save**.
2. Log in to MiVoice Connect Contact Center Director:
   a. Go to **Supervisors** > **Accounts** and remove the Agent from the Supervisor account.

   > **Note**:
   >
   > You might get a warning that the username must match.

   b. Set the Supervisor Username to match the Agent Username (AD login)
   c. Click **Save**.
   d. Re-assign the Agent Name back to the Supervisor.
   e. Click **Save**.
3. Have the Supervisor log in to a Supervisor application (such as Agent Manager, Reports, and so on.).
4. Go back to MiVoice Connect Director and navigate to **Administration** > **Users** > **Users**.
5. Select the user and check **Active Directory User**.
6. Click **Save**.

4.3.9.2 Scenario 2

For **Supervisors who are Agents, are AD enabled, and whose Agent Email Address was not set to the Client Username (that is, corporate email address) prior to the migration:**

1. Log in to MiVoice Connect Director:
   a. Verify the Client Username of the Supervisor by navigating to **Administration** > **Users** > **Users**. Select the user and click **Show from AD** or **Sync from AD**.
   b. Turn off AD Integration for the user.
   c. Click **Save**.
   d. Manually set the **Client Username** to match what the AD Client Username returned in step 1a above.
   e. Click **Save**.
2. Log in to MiVoice Connect Contact Center Director:
   a. Go to **Supervisors** > **Accounts** and remove the Agent from the Supervisor account.

> **Note**:
>
> You might get a warning that the username must match.

   b. Click **Save**.
   c. Go to the Supervisor's “Agent” record and set the **Agent Username** to be the AD enabled **Client Username**.
   d. Click **Save**.
   e. Go back to Supervisors and set the **Supervisor Username** to match the **Agent Username** (AD Login).
   f. Click **Save**.
   g. Assign the agent name back to the supervisor, and click **Save**.
3. Have the Supervisor log in to a Supervisor application (such as Agent Manager, Reports, and so on.).
4. Go back to MiVoice Connect Director:
   a. Navigate to **Administration** > **Users** > **Users**.
   b. Click **Save**.

4.3.9.3 Scenario 3

For **Supervisors who are Agents and are not AD enabled:**

1. Log in to MiVoice Connect Director.
2. Navigating to **Administration** > **Users** > **Users** and document the Client Username of the Supervisor.

> **Note**:
>
> This should have been completed in Step 12 of Prepare for the Migration.

3. Log in to MiVoice Connect Contact Center Director:

   a. Go to **Supervisors** > **Accounts** and remove the **Agent** from the Supervisor account by selecting **Not Defined** in the drop-down list.
   b. Click **Save**.
   c. Go to the Supervisor's “Agent” record and by navigating to **Agents** > **Agents** and selecting the **Agent Name**. Set the **Agent Username** to match the **Client Username** documented in Step 2.
   d. Click **Save**.
   e. Go back to **Supervisors** > **Accounts** and select the Supervisor record. (You might see a warning message: `Agent with username exists.`) Assign the **Agent Name** to the Supervisor account by clicking the drop-down list and selecting the **Agent**.
   f. Click **Save**.

4.3.10 Update Agent Desktop Application

1. Uninstall Agent Toolbar from the each agent’s system.
2. Browse to **http://<FQDN** or **IP of CC Server>:3000/ecc** for access to the **Agent Interaction Center**.

4.3.11 Update Supervisor Desktop Application

Note:

You do not need to uninstall previous versions of the Supervisor desktop application before installing the latest version.

1. Copy the **Connect Contact Center Supervisor**folder to the system that the supervisor will be using.
2. Run the **setup.exe**.

4.3.12 Set Client Timezone

In a MiVoice Connect Contact Center implementation, the time zone and Daylight Savings Time (DST) setting used by client applications, such as Agent Manager, should match the MiVoice Contact Center server time zone and DST setting.

To configure the client time zone and DST settings:

1. Launch **MiVoice Connect Contact Center Director**.
2. Navigate to **System Parameters** > **Client Preferences**.
3. Set the appropriate time zone and DST settings.

4.4 Important Migration Considerations

Refer to the following sections for important information to understand about the migration.

4.4.1 Ensure that the Starter Account Exists

The starter account, ea, must be present before you back up your EEC9 system and migrate to MiVoice Connect Contact Center. This starter account allows administrators to log in to Contact Center Director to set up supervisor administrator accounts and to configure licenses. Verify that you can successfully log into Contact Center Director before proceeding with the upgrade.

4.4.2 Turn off Redundancy (If Enabled)

Before starting the upgrade on the Primary Contact Center Server, change your system to manual failover mode in Connect Contact Center Director. This prevents the primary server from restarting as faulty.

4.4.3 Syncing Data Between PBX and Contact Center

Beginning with the MiVoice Connect PBX and MiVoice Connect Contact Center, the client username defined in the PBX must exactly match the agent username and supervisor username records defined in MiVoice Connect Contact Center.

If you need to make changes to ensure this information matches exactly, Mitel strongly suggests you make changes in MiVoice Connect first. If you need to make changes in the MiVoice Connect Contact Center to match what's defined in the PBX, you must restart the MiVoice Connect Contact Center service for the change to properly sync with the MiVoice Connect PBX database.

4.4.4 Update Agent Settings (Non-Supervisor)

If you configured email addresses for your agents in Enterprise Contact Center, be aware that the upgrade to MiVoice Connect Contact Center updates the Agent Username with this data and that this data might not match the user name defined for the agent in the MiVoice Connect PBX.

If the agent's email address is an external address, such as a Gmail or Yahoo address, it is not valid for use with MiVoice Connect Contact Center and must be modified.

If you do not have email addresses configured for your agents in ECC before you upgrade to MiVoice Connect Contact Center, be aware that the agent user name will be unspecified. You can add email addresses for all agents before upgrading, or you can add them after upgrading.

4.4.5 Extensions

Agent extensions, which are now a part of agent records in MiVoice Connect Contact Center, are stored in the MiVoice Connect Contact Center configuration database.

4.4.6 Update Supervisor Settings

To enable supervisors to have access to the Interaction Center to monitor agent interactions, you must assign an agent record to the supervisor.

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 MiVoice Connect PBX and MiVoice Connect Contact Center, the user's client username is what differentiates the record from other records, even if the record names match. For example, if you have two records for a person named Bob Smith, each record must have a unique user name.

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.

4.4.7 Class of Service

Agents must now be assigned to a Class of Service (COS) in MiVoice Connect Contact Center. If agents are not already assigned to a COS, they will be assigned to the Default COS in MiVoice Connect Contact Center, which has all COS features enabled by default.

Supervisor records in MiVoice Connect Contact Center now contain a user name, and you must manually enter the user name for each supervisor in MiVoice Connect Contact Center. This user name must exactly match what is defined for the supervisor user record in the MiVoice 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.

COS is also applied to services in MiVoice Connect Contact Center. For more information, see the ***MiVoice Connect Contact Center Administrator Guide***.

4.4.8 Configure KPI Boards for Agents

The KPI Boards feature allows you to configure the Interaction Center to include key performance information (KPI) about specific interactions. You can configure up to 12 different interaction metrics to include in the KPI Board.

For details on using KPI Boards, refer to the ***MiVoice Connect Contact Center Administrator Guide***.

4.4.9 CCIR Considerations

CCIR has a minor schema change with the release of MiVoice Connect Contact Center. This data now contains a value for the tenant record, but the tenant record is not used in MiVoice Connect Contact Center. The value of this record will always be zero. The tools that you use to consume and manipulate CCIR data will not need to be updated to handle the tenant record.

4.4.10 Re-install Brightmetrics (If Applicable)

Verify that you can run Contact Center Reports and that data is present.

If CCIR was moved to a separate server and Brightmetrics was running on the old server, follow the steps outlined in the following article to reinstall the Brightmetrics Agent on the new CCIR server:

https://brightmetrics.zendesk.com/hc/en-us/articles/210661243-Reinstalling-the-Brightmetrics-Agent

Migrating Mobility 8.x to Mobility 9.x 5

This chapter contains the following sections:

The following sections detail considerations and steps you must make before, during, and after the process of migrating your Mobility Router 8.x to Mobility 9.x.

Introduction

This document provides best practices in a time ordered procedure for the migration of the Mitel Mobility version 8 to Mitel Mobility 9.0.

You should upgrade Mobility after you migrate the ST14.2 PBX to MiVoice Connect, during the same maintenance window.

Refer to the following sections for information about upgrading Mobility 8.0 to Mobility 9.x.

5.1 Before You Upgrade

To prepare for upgrading the Mobility Router, perform the following preparatory steps in the weeks before the upgrade:

1. Review the Build Notes for the Mobility 9.x version.
2. Download the Mobility 9.x software from the Mitel support site.
3. Starting with Mobility Router build 9.1.11.107, Mobility licensing is handled through MiVoice Connect Director.

> **Note**:
>
> Ensure that the necessary Mobility licenses are present in MiVoice Connect Director.

4. Upload the Mobility 9.x software to the staging image of the Mobility Router. For details, see Upload the Mobility 9.x Software on page 64.

5. Verify that your organization's mobile devices and operating systems are supported by the Connect for Mobile apps by reviewing the following knowledgebase articles on the Mitel Support site:

   - Mitel Connect for iOS:
     - For Partners: https://mitelcommunity.force.com/partner/s/article/Mitel-Connect-for-iOS
     - For Customers: https://mitelcommunity.force.com/customer/s/article/Mitel-Connect-for-iOS
   - Mitel Connect for Android:
     - For Partners: https://mitelcommunity.force.com/partner/s/article/Mitel-Connect-for-Android
     - For Customers: https://mitelcommunity.force.com/customer/s/article/Mitel-Connect-for-Android

5.2 Install Mobility 9.x

Follow these steps to upgrade the Mobility Router to 9.x:

1. Perform an on-demand backup before you start the upgrade process. For details, see Perform an On-Demand Backup of the Mobility Router.
2. Upgrade the Mobility Router to the 9.x software. For details, see Upgrade the Mobility Router.
3. Open a browser and log in to the **Mobility Administration Portal**. Go to the **Configuration** > **Users** > **General** page and ensure that the **Local User** checkbox is not selected for users in groups.
4. Set up the directory to use the Trusted Admin App or the Bind User option. For details, see Configure the Directory.
5. Specify the authorization directory servers, as described in Specify the Authorization Directory Servers.
6. Install the Connect for Mobile apps. For details, see Install the Connect for Mobile Clients.

5.3 Detailed Installation Procedures

The following sections provide detailed procedures referenced from the high-level upgrade process.

5.3.1 Upload the Mobility 9.x Software

Mobility Router images can be installed from a local file system or using HTTP, SCP, or FTP.

The Mobility Router contains two hard-drive partitions. The Mobility Router Images page provides information about Mobility Router images that have already been installed and options to upload a new Mobility Router image from a URL or local file.

1. In the Mobility Administration Portal, go to **Maintenance** > **System** > **Images** > **Mobility Router**, and select one of the following:
   - **Select From URL:** Type the hostname, select the protocol, and enter the path of the server on which the Mobility Router Image is installed. If using FTP or SCP, a User ID is required. If using FTP, the FTP server must be running for the upload to succeed.
   - **Select From local file:** Select to install the Mobility Router image from a local file system or click **Browse** to navigate the file system. Select the Mobility Router image (*.img), and click **Open**.

> **Note**:
>
> If you are uploading the Mobility Router image from a local file system, you must use the Microsoft Internet Explorer Web browser

2. Click **Install**. The image is uploaded to the Mobility Router and is available to install.

5.3.2 Perform an On-Demand Backup of the Mobility Router

1. In the Mobility Administration Portal, click **Maintenance** > **System** > **On Demand Backup**.
2. Enter the **Hostname** or **IP address** of the location to send the configuration file.
3. Select the Protocol by which to send the file: **FTP**, **SCP** or **TFTP**.
4. Enter the Port number.
5. Enter the User ID. The entry must match the User ID for the selected server (FTP/SCP/TFTP).
6. Enter the Password for the User.

7. In the **Path** field, type the path to the directory and the filename to which you want to save the configuration file, for example: `/home/user/backup/test.bak`.

> **Note**:
>
> The FTP or TFTP server must be running for the backup to succeed.

8. Select **Backup**.
9. Verify that the **Backup Succeeded** message is displayed.

5.3.3 Upgrade the Mobility Router

To upgrade the Mobility Router, you must specify the new image for the upgrade.

1. In the Administration Portal, click **Maintenance** > **System** > **Images** > **Mobility Router**.
2. Select the image to be used at the next reboot.
3. Click **Set Next Boot**.
4. Click **Reboot**.
5. After the Mobility Router is restarted, log in and verify that the system software image has been updated.

5.3.4 Configure the Directory

Complete the steps in the following sections to set up connection configurations between the MiVoice Connect PBX and Mobility Router 9.x.

Two methods are provided:

- For a secure certificate connection, use the procedure in Configure the Directory to Use the Trusted Admin App (Recommended Method). This is the recommended method.
- To use the Bind User option, use the procedure in Configure the Directory with the Bind User Option.

5.3.4.1 Configure the Directory to Use the Trusted Admin App (Recommended)

1. In a command prompt window, run the following command:
   - `C:\Program Files (x86)\Shoreline Communications\ShoreWare Director\App\bin" pki.bat -S SMRAdminApp`
2. To generate the certificate for the Mobility Router, locate the following certificate and key files in the Shoreline Data\keystore\certs directory and copy their contents:
   - `SMRAdminApp.crt`, located in cert folder
   - `SMRAdminApp.key`, located in private key folder
3. Log in to Mitel MiVoice Connect Director and navigate to **System** > **Security** > **Trusted Server Application**.
4. Click **New**.
5. Specify the Trusted account name. This name, which is for reference only, should be a descriptive name that conveys the location and use of the Mobility Router.
6. Browse to **Shoreline Data\keystore\certs**, and select the **SMRAdminApp** file.
7. In the **Application Type** field, select **Client Application Service** and select **Enabled**.
8. In the **Property Type** field, select **admin-cas** in the **Available** list, and then click to move it to the **Selected** list.
9. Click **Save**.
10. Open a browser and navigate to the Mobility Router configuration page with administrator permissions.
11. Navigate to **Configuration** > **System** > **Authentication** > **Directory**.
12. Click **Add**.
13. In **Server Type**, select **ShoreTel Directory**.
14. Specify a Name.
15. Click **Apply**.
16. In the **Server Address** field, specify the headquarters FQDN or IP address.
17. Select **Trusted Admin App**, and then click the **Manage App Certificate** link to launch the **Directory Server Certificate** page.
18. Click **Import**, and paste the contents of the cert and key files you copied in step 2 of this procedure.
19. Click **Import** again, and then cancel the prompt to reboot.
20. In the **Security type** field, select **tls**.
21. Click **Apply**, and then click **Verify**.
22. Open a browser and navigate to the Mobility Router configuration page with administrator permissions.
23. Navigate to **Configuration** > **System** > **Authentication** > **Directory**, and select the directory you defined earlier in this procedure.

5.3.4.2 Configure the Directory with the Bind User Option

1. Open a browser and navigate to the Mobility Router configuration page with administrator permissions.
2. Navigate to **Configuration** > **System** > **Authentication** > **Directory**.
3. Click **Add**.
4. In the **Server Type** field, select **ShoreTel Directory**.
5. Specify a Name.
6. Click **Apply**.
7. Specify the Headquarters server FQDN or IP address in **Server Address**.
8. Enter a system administrator's credentials in **Bind User** and **Bind Password**.

> **Note**:
>
> Ensure that the credentials match the updated credentials in Connect Director that were updated after the migration to MiVoice Connect. You can use the Query option to search for a known directory administrator user name and to verify that you can successfully access the MiVoice Connect directory.

9. Select **tls** in **Security type** to configure a secure connection between the Mobility Router and the MiVoice Connect PBX.
10. Click **Verify** to verify the credentials against the server you specified in **Server Address**.
11. Click **Sync ABC Keys**. A pop-up message indicates that the synchronization was successful.

5.3.5 Specify the Authorization Directory Servers

> **Note**:
>
> Automatic user creation is not applicable to the Mitel Connect directory.

1. Open a browser and navigate to the Mobility Router configuration page with administrator permissions.

2. Navigate to the **Configuration** > **Groups** and **Users** page.
3. For External User Authentication/Authorization, select Mitel Directory and select the directory configured in Configure the Directory.
4. Click **Next**.
5. Complete configuration as necessary, and then click **Apply**.
6. Log out of the **Mobility Router** administrative portal, and then log back in again.

5.3.6 Migration Considerations

Authentication

Active Directory is not supported in Mobility 9.x. If Active Directory was configured previously, you should remove it. Authentication is provided through the Trusted Admin App configuration method described in Configure the Directory to Use the Trusted Admin App (Recommended Method).

5.3.6.1 Video

The video feature on the Connect for Mobile clients is not integrated with the Connect client on the desktop; you cannot make a video call between these two client applications.

5.3.7 Install the Connect for Mobile Clients

If you upgraded to Mobility Router 9.x, you must also upgrade clients to the current version of Connect for iOS available in the Apple App Store or Connect for Android available in the Google Play Store.

Refer to the following Knowledgebase articles on the Support website for details about these apps:

- Mitel Connect for iOS:
  - For Partners: https://mitelcommunity.force.com/partner/s/article/Mitel-Connect-for-iOS
  - For Customers: https://mitelcommunity.force.com/customer/s/article/Mitel-Connect-for-iOS
- Mitel Connect for Android:
  - For Partners: https://mitelcommunity.force.com/partner/s/article/Mitel-Connect-for-Android
  - For Customers: https://mitelcommunity.force.com/customer/s/article/Mitel-Connect-for-Android

After the Mobility migration is complete, users who are already using the Connect for IOS or Connect for Mobile apps should log out of the app and log in again. Users will be prompted to reset their passwords.