CHAPTER

1

Migrating the PBX

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

Refer to the following sections for migration details:

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**.

Before migrating, be sure to access the latest version of this document:

https://oneview.mitel.com/s/article/Mitel-Connect-ONSITE-Migration-Notes

You should be aware of some key differences between ST14.2 and MiVoice Connect. These differences are described in Migration Considerations on page 29. 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 OneView to access this article:

https://oneview.mitel.com/s/article/Feature-Comparison-for-ST-14-2-and-Mitel-Connect-ONSITE

PBX Migration Steps

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

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 see the "Migrating from 32-bit Windows Server to 64-bit Windows Server" section of the *ST14.2 Planning and Installation Guide* for details on this procedure.

4. 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.
5. Ensure that your ST14.2 installation uses the same install drive (for example, C:\ or D:\) that will be used for your MiVoice Connect installation.
6. Order SKU 30159, which supports the new MiVoice Connect licensing model, and apply the new licenses to Director. For details, see Licenses on page 29.
7. Confirm that any Mitel Professional Services applications are updated to versions that are compatible with MiVoice Connect.
8. Confirm that any third-party applications are updated to versions that are compatible with MiVoice Connect.
9. Ensure that all ST14.2 systems you are upgrading have current licenses that are in compliance.
10. 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 on page 16.
11. 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 release. If you have these voice switches, do not include them in the migration process.
12. Download the latest Connect software from https://oneview.mitel.com/s/article/Connect-Software and distribute it to all servers that will be upgraded.
13. Download the latest firmware for the 400-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 14.
14. 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.)
15. Run the Compatibility Checker on the DVSs and correct any errors.
16. If you have active directory (AD) integration configured, create a non-AD administrator account in Director.
17. 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.
18. Delete abandoned unplugged phones from Director.
19. Download Microsoft Updates as per the Connect Build notes. (In many cases these updates can be downloaded but not installed.)

20. 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.

21. Due to the schema change between MySQL 5.1 and MySQL 5.6, remove any customizations you defined for your CDR and restore the CDR to the default configuration before migrating. (After migration, you can re-implement the customizations.)

22. 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.

One Day Before the Upgrade

1. Download any recorded conferences from your service appliances. For details, see Recordings on page 30.

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.

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*.

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 details, see Back up the ST14.2 System on page 14.

2. If you use Enterprise Contact Center, back up the ECC application. For details, see Back Up the Enterprise Contact Center Components on page 38.

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 on page 15.

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 on page 15.

7. Disable Anti-Virus software and Windows Firewall on the HQ server.

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.

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.

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 on page 16. (Note that the DVSs will reboot.)

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 on page 17.

   e. Reconfigure the database reference for each Voicemail switch. For details, see Enable Distributed Database After Upgrade on page 16.

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. (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, etc.

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*.

Regenerate Certificates

- Regenerate self-signed certificates on any service appliances (SA-100/SA-400). For details, see Regenerate Self-Signed Certificates for Service Appliances on page 20.

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 on page 22.
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 on page 29 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, Chapter 2, Migrating ECC9 to MiVoice Connect Contact Center on page 34.
6. If you have Mobility, proceed with the Mobility upgrade during the same maintenance window. For details on the Mobility migration process, Chapter 3, Migrating Mobility 8.x to Mobility 9.x on page 48.
7. If you use Mitel for Salesforce, you need to perform some steps after the migration. For more information, see Mitel for Salesforce on page 32.

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 on page 21.

Required: Prior to making the certificate change to SHA256, verify all call functionality in the newly migrated Mitel MiVoice Connect system. For larger systems (1000+ users), best practices dictate four to five days of operation to confirm correct system functionality before rebuilding the certificates to use SHA256. For this reason, in many cases, the certificate change to SHA256 will require scheduling another maintenance window after the migration to complete the procedure.

Additional Details for Migration Sub-procedures

The following procedures provide details for some of the high-level steps included in PBX Migration Steps on page 8 and Day of the Upgrade on page 10.

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 https://oneview.mitel.com/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. Wait up to 5 minutes for the downloaded firmware to display in the Diagnostics and Monitoring interface in Director.
6. Click **Maintenance > Diagnostics & Monitoring**.

   The Dashboard page is displayed.
7. Navigate to **Status > IP Phones**.

   The IP Phones page is displayed.
8. Select the check box for each phone to which you want to download the firmware.
9. In the **Command** drop-down menu, select **Download**.
10. Click **Apply**.
11. In the Confirmation dialog box, click **Advanced**.
12. For each type of phone selected, in the **Version** drop-down list select the firmware version that corresponds to the firmware you downloaded.
13. Click **OK**.

Back up the ST14.2 System

1. 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
```

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. Backup the Web Bridge database on the HQ server using the following command:

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

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:
   - Prompts
   - Vms
   - UserData
   - Keystore
7. Back up the following folders from the Shoreline Data folder on each DVS:
   - Vms
   - UserData
   - Keystore

Disable Active Directory (AD) Integration Before Upgrade

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

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

Disable Distributed Database Before Upgrade

Disable distributed database 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 the 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**.

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**.

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 n 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 command `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 n the Diagnostics and Monitoring system and checking the value in the **Boot ROM Version** field on the Status tab.

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

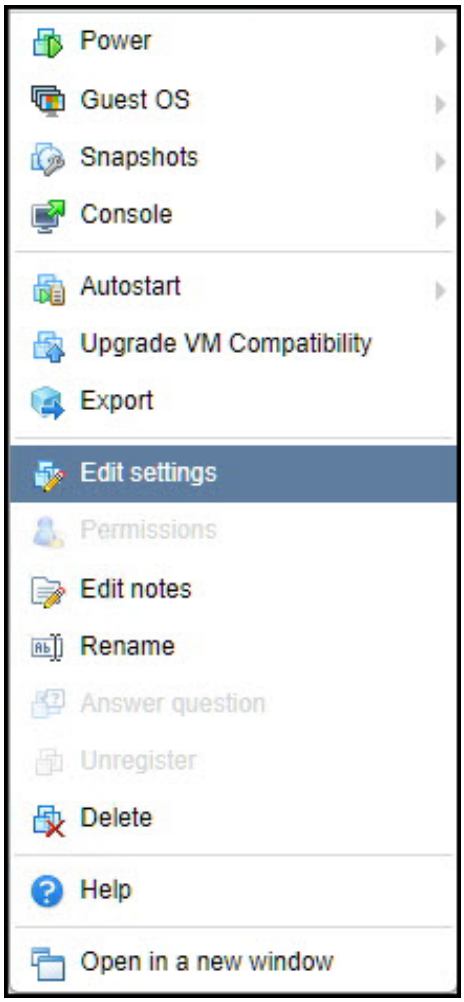
Be aware that selecting the check box to apply an upgrade to all appliances in the **Maintenance > Status and Maintenance > Appliances** page selects only the appliances on that page. If you want to upgrade more appliances than those shown on a page, you must manually select additional appliances on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

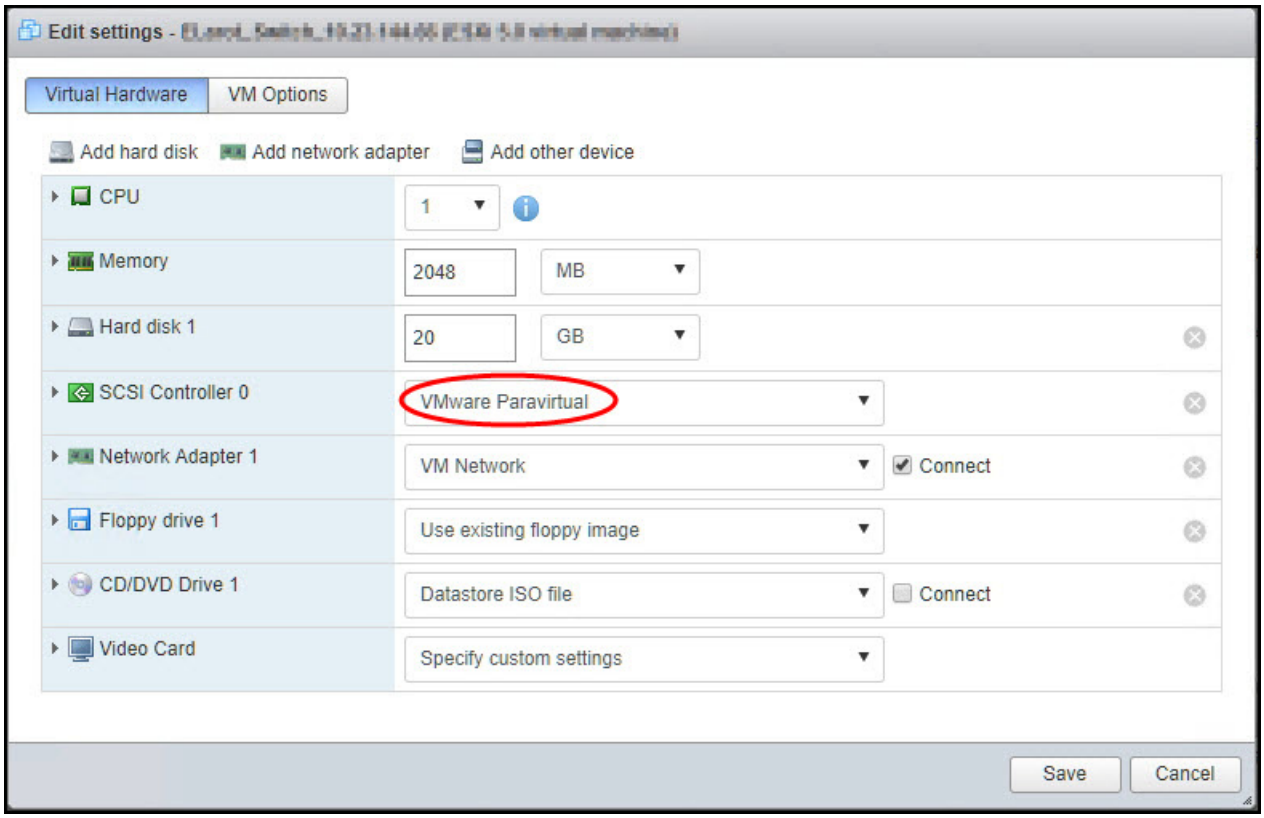
   Warning: dracut-initqueue timeout – starting timeout scripts

   Entering emergency mode. Exit the shell to continue

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



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



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**.
   d. Type **1** to select **Show version**.

      The **Release version** and **Program version** detail appears.

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** drop-down 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** drop-down 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.

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. (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

   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. On 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 may 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 on page 22.

9. Confirm that all phones are working.

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. On 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.

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.

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.

CDR Offline Migration

Due to the schema change between MySQL 5.1 and MySQL 5.6, the Connect installer prompts you to take a back up of your CDR prior to beginning 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.

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 on page 15:

   - 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 on page 15, 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 5.1 and ODBC drivers on the secondary archive server using the Control Panel.

2. Check <installation location>\MySQL\MySQL Server 5.1\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 MySQL5.6 (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 where MySQL Community Server 5.6.25 is to be installed.

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.

a. 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:

- If you are running Windows Server 2008 R2 (Enterprise or Standard Editions only) (64-bit version) with or without SP1, you must install the .Net Framework 4.0.
- 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 MySQL5.6 (64 bit) on the Secondary Server on page 24.
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\MySQLCDR\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`.

Tip

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 5.6\Dat\ ib_logfile*` file where the asterisk represents a wildcard.
8. In the `<installation location>\MySQL\MySQL Server 5.6\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 on page 22.

      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 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.

Reconfigure Extensions for Recording Auto Attendant Prompts and Workgroup Names

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**.

Migration Considerations

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

Licenses

All licenses and related functionality already installed on the ST14.2 system are carried over to MiVoice Connect during the migration process.

If you are a licensed Personal Access user, be aware that the softphone and video features of the Connect desktop client are provided in no-charge upgrade SKU 30159.

WARNING!

You must purchase the no-charge upgrade SKU 30159 to use the desktop client without entering the 45-day trial period and being subjected to lockout at the end of the trial period.

Additional Connect features are provided in bundles and licensed individually. Be aware that migrating to MiVoice Connect from ST14.2 does not include migrating to a MiVoice Connect bundle. Only those applications and features that were licensed in ST14.2 are activated after migrating to MiVoice Connect, with the exception of the softphone and video client features.

To take advantage of MiVoice Connect bundling and pricing advantages to add functionality beyond what you already had licensed in ST14.2, contact your Mitel representative about MiVoice Connect license bundles, related upgrades, and a la carte ordering.

Service Appliances

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

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 on **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.

Reservationless Conferences

Note

- The **Allow participants to IM** option is no longer available in MiVoice Connect. Therefore, please be sure 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.

Refer to 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.

Communicator

Be aware of the following behavior differences between Communicator and the Connect client.

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).

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.

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.

Call Routing Rules

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.

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.

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.

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 knowledgebase article:

https://oneview.mitel.com/s/article/Mitel-for-Salesforce-Migrating-from-ST14-to-Connect