Virtual Mobility Router Installation Guide

August 2024

This document describes the one-time installation procedure for the Virtual Mobility Router. The topics discussed in this document include:

Virtual Mobility Hardware

Recommended configuration for the Virtual Mobility Router is as follows:

- 4 cores
- 4 GB RAM
- 100 GB disk space
- 2 network interfaces
- The following interfaces where the Mobility Router is installed:
  - Eth0—Management VLAN. Requires a web service for admin portal, SSH, SNMP, Diagnostics and Monitoring in Director (D&M), Syslog, NTP, and SMTP. D&M shows information like call statistics, duration, numbers involved, and so on.
  - Eth1—External DMZ. The connection to SMC is through RAST.

Note

Only Virtual CMR supports Rocky Linux.

VMware Virtual Environment

The following versions of VMware are supported:

- VMware vSphere ESXi 6.x, 7.x.

Notes for VMware Support:

- High Availability and VMware vSphere vMotion are supported.
- Fault Tolerance is not supported. VMware does not support this feature across multiple CPUs.
- Snapshots are not supported. Snapshots can consume significant CPU and memory resources, impacting system operation.

Before You Begin

Before beginning the configuration:

- You must have the Mobility Router hostname.
- If you are not using DHCP, you must have the Mobility Router IP address, Subnet mask, Default Gateway, DNS server address, and domain name for the Mobility Router.

Note

Upgrading the CentOS-based Virtual CMR is not supported. A fresh install of the Rocky Linux-based Virtual CMR is required. Ensure to take a backup of the CentOS-based CMR and then restore the backup in the fresh install of the Rocky Linux-based CMR.

Installing the Virtual Mobility Router ISO

Follow the steps to create a new virtual machine for virtual Mobility Router Software:

- Creating New Virtual Machine in VMware or Hyper-V on page 3
- Configuring and Installing the Virtual Mobility Router on page 6

Note

The Virtual Mobility Router ISO must be installed on VMware version 6.5, 6.7, 7.0 and 8.

Creating New Virtual Machine in VMware or Hyper-V

Creating a new Virtual Machine in VMware

Before creating a new virtual machine in VMware, it is recommended to upload the ISO installer to the VMware datastore. The ISO installer is uploaded only once for a given build, and it can be reused for creating multiple new virtual machines.

To upload ISO Installer file to the vSphere Web Client ESXi 6.0 or 6.5, do the following:

1. Open the vSphere Desktop Client and log in to VMware ESXi server with valid credentials.
2. Navigate to **Home**, and click **Inventory**.
3. Click **Datastores and Datastore Clusters**.
4. On the **Datastores and Datastore Clusters** tab, select the datastore to which you want to upload the ISO installer file.
5. Right-click the datastore and select **Browse Datastore**.

   The **Datastore Browser** window appears.

6. (Optional) Select the root folder and click **Create a new folder** icon from the menu bar, type the required name, and click **OK**.
7. Select the folder that you created or select an existing folder, and click **Upload a File** icon from the menu bar, and select **Upload File**.
8. Click **Browse** and select the virtual Mobility Router iso file from your local drive or location, and click **Next**.

   Time required to upload the ISO installer file varies, depending on the file size and the network upload speed.
9. In the confirmation dialog box, click **Yes**.

   Refresh the datastore file browser to verify the uploaded ISO installer file is in the list.

To create a new virtual machine in VMware:

1. Connect to the VM blade through a web browser.
2. In vSphere Web Client, click **Create/Register VM**.

   The wizard to set up a new virtual machine is displayed.
3. In the wizard, select **Create a new virtual machine**, and then click **Next**.
4. Enter a name for the new VM (for example, cmr01), and select the following options in the other fields:
   - In the **Compatibility** field, select **ESXi 6.0 virtual machine**.
   - In the **Guest OS family** field, select **Linux**.
   - In the **Guest OS version** field, select **CentOS 8 (64-bit)**.
5. On the Select storage page, select the destination datastore for the new VM, and click **Next**.
6. On the Customize Settings page and the Virtual Hardware tab, select values for the options as follows:
   - In the **CPU** field, select **4**.
   - In the **Memory** field, select **4096 MB**.
   - In the **Hard disk 1** field, select **100 GB**.
   - In the **SCSI Controller 0** field, select **VMware Paravirtual**.
7. Ensure that **Network Adapter 1** is attached to an internal network.
8. Click **Add network adapter**, and for the second network adapter select an external/DMZ network.
9. Click **Add other device**, and select **CD/DVD drive**.
10. In the **New CD/DVD Drive** field, select **Datastore ISO file**.

11. In the Datastore browser window, highlight **CMR-<*w.x.y.z*>.iso**, and click **Select**.

Note

This ISO file was included with the CMR image and OVA file. You might need to upload this ISO file so that it is available to be selected in the list.

12. Click **Next**, and review the details. Ensure that the **Provisioning** field is set to **Thin Provisioned**.
13. Click **Finish**.
14. Select the new VM from the list of VMs, and click **Power on**.

Creating a Hyper-V Standard and Standalone Virtual Machine

To create a virtual machine in Hyper-V:

1. On the **Hyper-V Manager**, right-click **HYP-V,** and click **New**.
2. In the pop-up menu, select **Virtual Machine**. The **New Virtual Machine** wizard appears.
3. On the **Specify Name**, and **Location** tab, type the required virtual machine name, and click **Next**.
4. On the **Specify Generation** tab, select **Generation 1,** and click **Next**.
5. On the **Assign Memory** tab, type the memory size allocate for the virtual machine:
   - Startup memory: 4096 MB (4 GB).
6. Click **Next**. The **Configure Networking** tab appears.
7. On the **Connect Virtual Hard Disk** tab, type the virtual hard disk size:
   - Size: 100 GB.
8. Click **Next**. The **Installation Options** tab appears.
9. On the **Installation Options** tab, select **Install an operating system from a bootable CD/DVD-ROM**. Select **Image file (.iso).**
10. Click **Browse**, select the **Virtual Mobility Router ISO** file from the file location, and click **Next**.
11. In **Completing the New Virtual Machine Wizard**, verify the details you have entered, and click **Finish**. From the **Virtual Machines** list, right-click the newly created virtual machine, and do the following:
    a. Click **Start** to start the virtual machine.
    b. Click **Connect** to connect to the console.
12. After a few minutes, the installation process completes as indicated by the status bar. You must remove the **Virtual Mobility Router ISO** file selected in step 10. Switch-off the Mobility Router, remove the ISO file, and then switch-on the Mobility Router again. Once the Mobililty Router is switched-on, it will display a login prompt, which indicates successful installation.

Components Supported under Microsoft Hyper-V

Note

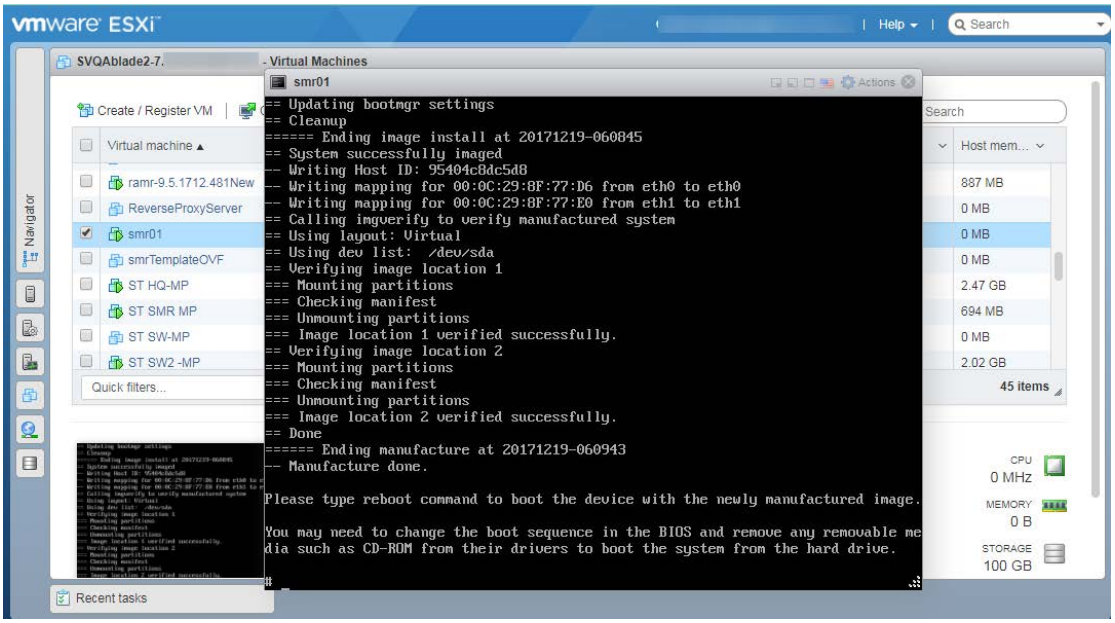
Microsoft Hyper-V Windows 2016 Generation 1 and Microsoft Hyper-V Windows 2019 Generation 1 are *only* supported.

Configuring and Installing the Virtual Mobility Router

1. After the VM is turned on, select **Console**, and in the drop-down list select **Open browser console**.
2. The virtual machine boots from a bootflop image. Enter the following command to manufacture the CMR image:

   ```
   cd /mnt/cdrom
   manufacture.sh -a -m mrVirtual -d /dev/sda -f /mnt/cdrom/image.img
   ```

3. After a few minutes, the installation process completes, and the CMR reboots and displays the **login** prompt. A successful installation generates messages similar to the following:



4. As prompted, type **reboot** and press **Enter**.

   The system reboots, which takes a few minutes.

5. At the **login** prompt, log in as “admin”. (No password is required.)
6. At the next prompt, type **Enable** and press **Enter**. At the next prompt type **_crusto** and press **Enter**.
7. At the next prompt, type **wizard** and press **Enter**.
8. At the **Hostname** prompt, enter the VM name you specified in step 4 (for example, cmr01).

9. At the **Use DHCP on eth0 interface** prompt, type **No**.
10. Enter the Primary IPv4 address and masklen (0.0.0.0/0), for example 10.23.174.100/24.
11. Enter the default gateway (0.0.0.0).
12. Enter the primary DNS server address.
13. Enter the domain name.
14. Enter a new strong Admin password. Passwords should not be left at default and should meet the customers password security policy, for example, complexity, length, and so on.
15. Enter a new strong Monitor password (if monitor account exists). Passwords should not be left at default and should meet the customers password security policy, for example, complexity, length, and so on.
16. If you need to edit any of the parameters you've just entered, type the step number to edit that parameter. Or press **Enter** to save changes and exit.
17. At the next prompt, type **reboot** and press Enter.

Note

When the system needs to be redeployed, then in Steps 14 and 15 you must enter new strong passwords for the Admin and Monitor (if exists) accounts.

After the reboot, the CMR is successfully deployed.

The Virtual Mobility Router is now ready to be configured using the Administration Portal. For more information on configuring and maintaining the Mobility router, refer to the *Mobility Router Administration Guide*.

Note

The Admin users have root privileges and entering **_crusto** provides the admin user root level CLI access.

Note

For information about installing CMR behind a firewall, see the Mitel Connect Mobility Router Integration Guide for Mitel MiVoice Connect document in the doc center.

Installing the Virtual Mobility Router OVA

Note

The Virtual Mobility Router OVA must be installed on VMware version 5.1 or higher.

1. Log in to VMware ESXi server.
2. Select **File > Deploy OVF Template**.
3. Enter the path to the Mobility Router OVA/OVF.
4. Enter, or copy/paste the URL to the web source of the OVA/OVF. Click **Next**.

   or
5. Click **Browse,** and select **the OVA/OVF** from your local drive/location. Click **Next**.
6. On the OVF Template Details page, click **Next**.
7. Select **Open** and follow the prompts. Change the name if desired and note this name for configuring the DVS server later, and choose the options best suited for your environment.
8. Enter the virtual machine **Name** and select the inventory location. Click **Next**. The Storage page opens.
9. Select the host or cluster on where you want to deploy the virtual Mobility Router and click **Next**.
10. Select the destination storage for Virtual Mobility Router files. Make sure that the required disk space is available on the destination storage. Click **Next**. The Disk Format page opens.
11. Check the **Thick Provision Lazy Zeroed** check box. Click **Next**. The Network Mapping page opens.
12. Map the networks used in the OVF template to network in MiCloud inventory. Click **Next**. The Ready to Complete page opens.
13. Check the **Power on after deployment** check box. Click **Finish**.

    The vSphere client loads the virtual Virtual Mobility Router and installs it on the vCenter server. After the installation is complete, the virtual Virtual Mobility Router appears in a powered-on state in the vSphere client.
14. Open the vCMR console.
15. At the login prompt, type **admin** in the Username field and click **Enter**.
16. A pop-up to accept the **End User License Agreement** appears. Click **YES** to accept the end user license agreement. The initial configuration wizard opens.
17. Enter **Y** to proceed with the configuration using the wizard.
18. Enter the **DNS hostname** of the Mobility Router. The hostname can be in short-name format or fully qualified domain name (FQDN).

19. At the **Use DHCP on ETH0** interface prompt, Enter **NO**.
20. Enter the Mobility Router's **Primary IP address**. IP addresses on other interfaces are configured through the Admin portal.
21. Enter the **Subnet Mask**.
22. Enter the **IP Address** of the default gateway for the Mobility Router.
23. Enter the **IP Address** of the primary DNS server.
24. Enter the **domain name** in the format domain-name.com.
25. Assign a strong password to the default Admin account for future access to the Mobility Router Administration Portal.
26. Confirm the password for the default Admin account.
    After completing the initial configuration wizard, a summary list appears. Verify the information and click **Enter** to save the configuration.
27. At the prompt, click **Enable**.
28. Enter **reload** to restart the Mobility Router. Wait for the login prompt in the terminal emulation software window, which indicates that the Mobility Router has finished restarting.
29. Verify a network connection to the Mobility Router by accessing the Administration Portal. To access the Administration Portal, enter the Mobility Router hostname or IP address in a Web browser:

    To access the Administration Portal:

    a. Using a Web browser, enter the IP address or hostname of the Mobility Router in the address bar using the following format:

       `https://Mobility-Router-address/admin`

       where *Mobility-Router-address* is the IP address or fully qualified domain name (FQDN) of the Mobility Router (for example, https://10.11.12.13/admin or https://sj.example.com/admin).

    b. Type the username and password, and click **OK**.
30. After verifying the access to the Administration Portal, disconnect the console connection via the hypervisor (Console access is no longer required).

Configuring Ethernet Interfaces

After specifying the basic Ethernet interface in the Initial Configuration Wizard, you can configure the following settings for the Ethernet interface (eth1):

- Interface speed
- Duplex settings

Some information in the fields under the Interface menu reflect the responses provided during the Initial Configuration Wizard setup. Some fields are set to system defaults that generally do not require changing.

- eth1—Configure an IP address from external DMZ. The SMCs connect to this IP address through RAST.

1. Click **Configuration > System > Networking > Interface**. The Interface page displays.
2. Click eth1. You can enable or disable the interface.
3. Enter the **Static IP Address** and **Gateway**.
4. Enter the **IP Address**, **Subnet mask**, and **Gateway** address in their respective fields.
5. For eth1 interfaces, we need to enter the Gateway address along with IP address and network mask.
6. Verify the interface speed. The default and recommended value is **Auto**. To change the speed, select one of the following in the Speed list:
   - 10—10 Mbps
   - 100—100 Mbps
   - 1000—1000 Mbps
   - Auto—Speed is auto-detected
7. Verify the duplex value. The default value is **Auto**. To change the duplex setting, select one of the following in the Duplex list:
   - Full—Full-duplex
   - Half—Half-duplex
   - Auto—Auto-detect duplex setting.
8. Review the MTU value.
9. Verify the MAC address.
10. Review the online Status of the Mobility Router.
11. To save your changes, click **Apply**.

Updating Remote Access FQDN and Public NAT IP

1. Click **Configuration > System > Networking > Remote Access**.

   The **Remote Access** page displays with the **General** tab active.

2. To enable remote access, make sure the **Enable** check box is selected. By default, this check box is not selected.

3. In the **Remote Access IP Interface** list, select the Ethernet interface used for remote access. Typically, this is the eth1 interface.

4. To establish a secure remote connection from an external network, enter a valid FQDN in the **Remote Access FQDN** field.

5. In the Public NAT area, configure the following:

   - To enable a public network address translation (NAT) IP address for the Mobility Router, make sure that the **Enable** check box is selected. By default, this check box is selected. To disable the NAT IP address, clear the **Enable** check box.
   - In the **IP Address** field, type the external IP address used for NAT.
   - In the **UDP Port** field, type the port number for the external IP address to which clients connect. The port number can be between 80 through 49151. The default value is 443.
   - In the **TCP Port** field, type the port number for the external IP address to which clients connect. The port number can be between 80 through 49151. The default value is 443.

6. Click **Apply**.

Importing Local Access Certificate

1. Click **Configuration > System > Certificate > Mobility Router > Standalone > Local Access**.

   The **Local Access** page displays.

2. Click **Import**.

   The Import Certificate page displays.

3. In the Import area, **paste** the Certificate.

4. Click **Apply**.

Importing Remote Access Certificate

1. Click **Configuration > System > Certificate > Mobility Router > Standalone > Remote Access**. The **Remote Access** page displays.
2. Click **Import**. The Import Certificate page displays.
3. In the Import area, **paste** the Certificate.
4. Click **Apply**.

Generating and Installing SIP TLS Certificate

To generate and install the SIP TLS certificate, do the following:

- Generate a TLS Certificate on the PBX
- Configure the CMR

Generating a TLS Certificate on the PBX

1. On the HQ Machine, click **Run**.
2. Type **cmd** and press **ENTER**.
3. Type **cd C:\Program Files (x86)\Shoreline Communications\ShoreWare Director\App\bin** and press **ENTER**.
4. Execute the following command by providing IP address of the CMR: pki.bat –s IP_Address_of_CMR (For ex. IP Address on my CMR is 10_23_223_50)

The following two certificates are generated for SRTP:

- C:\Shoreline Data\keystore\certs named as 10_23_223_50.crt and
- C:\Shoreline Data\keystore\private named as 10_23_223_50.key

Configuring CMR

1. Click **Configuration > Voice > IP PBXs**.
2. Click **Add**.

   The Add IP PBX page displays.
3. In Line-Side Support area, do the following:

   a. From the SIP Transport drop-down list, choose **TLS**.

   b. Click **Import** next to the **Certificate** field.

c. Enter the SRTP Certificate ID.

d. Enter the hq_ca.crt in the HQ CA Root Certificate area. (The hq_ca.crt is stored in C:\Shoreline Data\keystore\certs.)

e. Enter the SRTP TLS Certificate in the SRTP TLS Certificate area. (The SRTP TLS Certificate is stored in C:\Shoreline Data\keystore\certs.)

f. Enter the SRTP TLS Private Key in the SRTP TLS Private Key area. (The SRTP TLS Private Key is stored in C:\Shoreline Data\keystore\private.)

4. Click **Import**.

Creating a Mitel Directory Server

The following procedure configures a Mitel Directory Server:

1. Click **Configuration** > **System** > **Authentication** > **Directory**.
2. Click **Add**.
3. Select **ShoreTel Directory** from the Server Type drop-down list.
4. Enter a **Name**.
5. Click **Apply** to advance to the Add New Directory Group parameters page.
6. Enter a fully qualified domain name (FQDN) for the Mitel HQ server in the **Server Address** field.
7. In the **Server Port** field, use the default port number.
8. Select the **Sky cluster** check box. Enter the FQDN server address in the **ABC server address** field.
9. Choose **TLS** from the Security Type drop-down list.
10. Use the default **Secure Port** value, 5448 (CAS secure port).
11. Select the **Trusted Admin App** check box.
12. Click the **Manage App Certificate** link to view and import the Trusted App certificate. A new window opens. A new API is provided for CAS to utilize the more efficient permanent connection to the Mobility Router. One connection is used for all users.
13. Click **Import.** Copy and paste the appropriate Trusted App Certificate. Paste the Trusted App private key. The encrypted key is not accepted.
    The certificate must be enclosed within the following tags:

    ```
    -----BEGIN RSA PRIVATE KEY-----
    ```

    and

    ```
    -----END RSA PRIVATE KEY-----
    ```

14. Click **Apply** to save the directory configuration.
15. Click **Verify** to verify the directory server configuration is correct.
16. When the certificate verification is enforced, the Mobility Router verifies the following:
    - The certificate is valid and not expired or damaged.
    - The subject name or the first name in the Subject Alternative Name (SAN) matches with the Fully Qualified Domain Name (FQDN) of the Mitel Directory server.
    - It was issued by the trusted authority, and a certificate chain can be established up to the hq_ca certificate imported before.
17. Click **Sync ABC Keys** to exchange the authenticator public keys with Mitel HQ and DVS servers.

Note

If verification or sync fail, login to HQ/D2 server, and start the Shoreware Client Application Services. Click Sync ABC Keys.

18. Create External User Authorization enabled CMR group for the tenant.
19. Choose Mitel Directory to map the Mobility Router group to a Mitel Directory. Choose the appropriate one from the drop-down list as “Directory Search Group” and “Authorization Directory”.
20. Click **Apply**.
21. Create the external CMR user (user@domain) for the tenancy group, which activates the CMR service to HQ bootstrapper database automatically. For the existing users, you can activate the HQ bootstrapper by enabling them.

Configuring Support Service

Click **Configuration** > **System** > **Support Service** to enter a Support email and phone number for Mitel Connect users.

When “Call Support” is initiated by the user on the Mobility app, the phone number entered here is called. If the user opts to select “send log”, the information is sent to the email address entered here.

Migrating CMR from VMware to Microsoft Hyper-V Infrastructure

This section describes how to migrate your existing CMR from VMware to Microsoft Hyper-V Infrastructure.

Backing up the CMR

Procedure to back up MR:

1. Log in to the Connect Mobility Router with the administrator access.
2. Navigate to **Maintenance > System > On Demand Backup**.
3. On the **On Demand Backup** page, do the following:
   a. Type **Hostname** or the **IP Address** of the location to which you want to send the configuration file.
   b. Select Protocol: **scp**
   c. Type Port: **22**
   d. Type the **User ID** and the **Password** that match the Hostname credentials.
   e. In the path field, type the path of the directory or the file name where you want to save the configuration file.

      For example, /home/admin/backup/sample.bak.
   f. Click **Backup**.

      The status of the Mobility Router backup is displayed. A notification appears when the backup is complete.
   g. Log in to the Host that you have created.

      For the successful completion of the backup procedure, ensure that the backup files are created in the specified location.

Restoring CMR on Hyper-V

1. Create a new virtual machine in the Microsoft Hyper-V infrastructure for CMR, similar to that of the VMware infrastructure. For example, CMR build, ISO file, and the same network configuration.

   Refer to the Installing the Virtual Mobility Router ISO on page 3 for information about creating a new virtual machine in Hyper-V infrastructure.
2. Log in to the Connect Mobility Router with the administrator access.
3. Navigate to **Maintenance > System > Restore**.

4. On the **Restore** page, do the following:

   a. Type **Hostname** or the **IP Address** of the location to which you want to send the configuration file.

   b. Select Protocol: **scp**

   c. Type Port: **22**

   d. Type the **User ID** and the **Password** that match the Hostname credentials.

   e. In the path field, type the path of the directory or the file name from which you want to restore the configuration file.

      For example, /home/admin/backup/sample.bak.

   f. Enable the following:

      - Include License
      - Include Network Information
      - Include Certificates

   g. Click **Restore**.

      The status of the Mobility Router restore is displayed. A notification appears when the backup is complete.

5. Click **Exit** and restart the browser.

6. Log in to the Mobility Router with the administrator access.

   For the successful completion of the restore procedure, ensure that the backup files are restored in the specified location.

Note

- After the migration, the CMR MAC address (**Mobility Router > Configuration > System > Interface**) gets changed; therefore, you must delete the existing license key, and then request for a new license key with a new CMR MAC address. You have 45 days to install the license key. After you add the new license (**Mobility Router > Configuration > license**), the state should be valid and active.
- IMs will not be synced after the migration.

Configuring CloudLink to enable Push Notifications

Prerequisites

Before configuring the CloudLink, you need to complete the below steps:

1. A CloudLink Customer Account and a verified CloudLink Account Admin User in that account must be created in order to associate the mobility users within CloudLink. Refer to the following link to create the Account and User credentials necessary to enable CloudLink.

2. CloudLink must be enabled in **MiVoice Connect Director (D2)**. Refer to the *CloudLink configuration* section under the *Setting Up System Parameters* chapter of *MiVoice Connect System Administration Guide*.

3. Connect Mobility Client (CMC) sends an API request to Connect Mobility Router (CMR) to get the basic configuration at port 4433. Based on the response from CMR, CMC determines the CloudLink integration status and whether push notification is supported or not. For the list of ports used by CMC and CMR, refer to *Appendix D - Port Usage table* (Originating Device: CMC, Destination Device: CMR) of the *MiVoice Connect Maintenance Guide*.

   Make sure the following requirements are met to ensure the push notification call works:

   Connect Mobility Router (CMR)

   A. Firewall should allow the TCP Port 4433 for CMR.

   B. Go to **Configuration -> System -> Cloudlink**, input the appropriate CloudLink info, and click the **Verify** button.

   The verification should be successful.

   If the verification fails, check the CloudLink admin account or check whether CloudLink is enabled in the Director.

   Connect Mobility Client (CMC)

   A. If the user does not want to use the push notification calls and the CloudLink configuration is disabled, then the user must logout and re-login.

   B. If the user wants to use the push notification calls and the CloudLink configuration is successful, then CMC displays the CloudLink Auth portal.

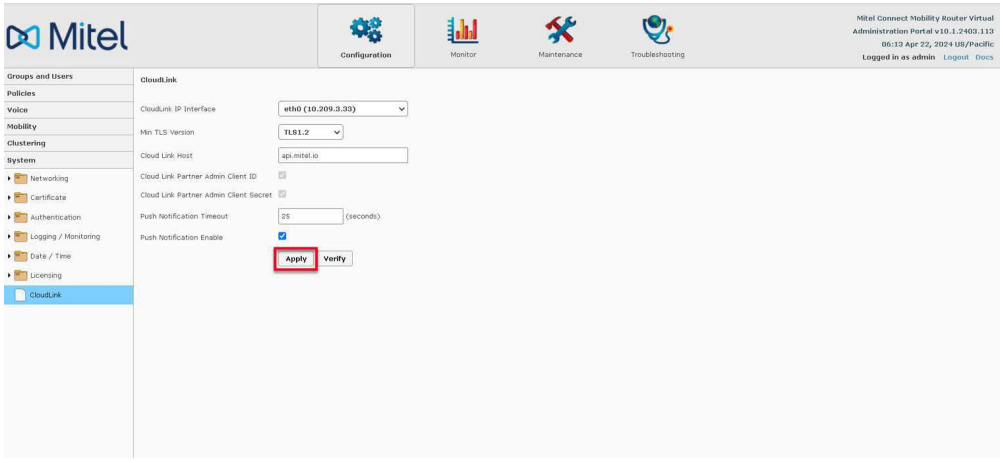
   If the CloudLink Auth portal is not displayed, recheck the CMR conditions (A and B).

Enabling Push Notification

Mobility client registers (SIP registration) with Mobility router for receiving events. However the application is suspended by the mobile operating system when its on the background and hence mobility client is unable to receive the real time events related to calls. Push notification will refresh the mobility client application and hence mobility client will be able to receive the calls all the time.

To enable push notification, perform the following steps:

1. Access the administration portal and navigate to **System** > **CloudLink**.
2. Select the internal interface for CloudLink IP Interface option.
3. Select **TLS 1.2** as Min TLS Version.
4. Enter **api.mitel.io** in CloudLink Host.
5. Select the check box **Push Notification Enable**.
6. For all other fields leave default values.
7. Click **Apply**.
   The administration portal navigates to the CloudLink Authentication portal.
   1. Enter the CloudLink credentials and click **OK**.
   2. Click on **Verify** to confirm the CloudLink integration status.



8. User accounts in CloudLink portal are automatically created once the **Enable enhanced mobility with extension** option is checked in D2.
9. For users which are already enabled with **Enhance mobility**, need to disable and enable again. The option “enable enhanced mobility with extension” needs to be 'enabled again' only after “enable CloudLink” step is completed.
10. Update the new mobility **Client ID** for all the users in the Mobility Router Administration portal.

11. It is mandatory for all the Users who are enabled with **Enhanced mobility with extension** to have valid email address. Welcome email containing “the link to build the CloudLink account” will be sent to the user’s email address. Users need to access the link and configure the password. If the user fails to receive the Welcome email, the Admin will need to manually send welcome emails to the user accounts that were created once the option “enable enhanced mobility with extension” is checked from D2. The CloudLink portal has the option to “send welcome emails” to verify the users to complete the onboarding process. Additionally, verified users can be sent Reset Password emails. See the “Managing Users” section in https://www.mitel.com/document-center/technology/cloudlink/all-releases/en/cloudlink-accounts-html.

12. Launch the mobility client and enter the user credentials. CloudLink Authentication portal opens up and the users need to enter the CloudLink credentials and then login to the mobility client application. The user is now configured to receive incoming calls even when the application is suspended by mobile operating system.

Incoming Call Alert

Once the Push Notification is enabled, the user will be able to receive an incoming call even when the mobile is idle for more than 3 minutes. Without the push notification, the call goes to voicemail.

Note

Push Notification will work only when the Mobility Client is connected using Public Network.

The following table describes the various incoming call alerts with screenshots after enabling push notifications on Android and iOS devices. The sample screenshots are provided for illustration purpose only.

Table 1: Incoming Call Alert - Normal & Push Notification

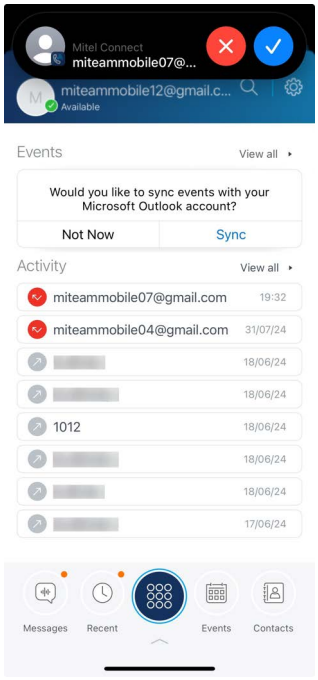
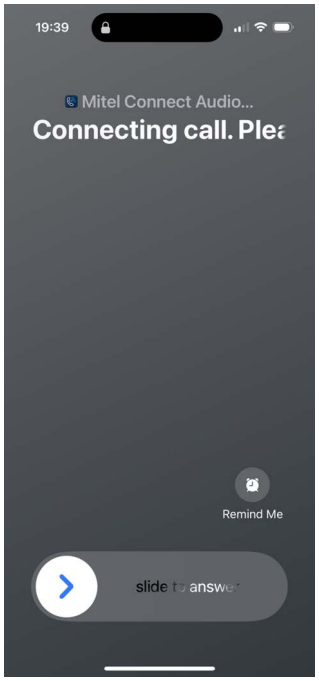
Alerts	Screenshot
Normal incoming call alert	

Table 1: Incoming Call Alert(Continued)- Normal & Push Notification

Alerts	Screenshot
Initial Incoming Call alert using Push notification	
Updated Incoming call alert using Push notification The notification is updated after the application processes the caller details, similar to a Normal incoming call alert.