Onboarding MRA Devices

MRA Device Onboarding via Activation Codes

Activation Codes provide a simple and secure way to onboard remote endpoints for Mobile and Remote Access (MRA). This feature eliminates the need for an MRA user to be on-premises the first time they use their phones. Remote users can plug in the phone, enter the activation code, and then start placing calls.

This feature leverages the Cisco cloud to handle onboarding. An administrator onboards Cisco Unified Communications Manager to the cloud, specifying the clusterwide MRA Activation Domain with the Expressway cluster to which all remote MRA users connect during device activation.

If you have multiple Expressway clusters, MRA Service Domains let you specify which Expressway your phones register. After the phone activates, the phone downloads its configuration file, which contains a redirect to the MRA Service Domain with the Expressway cluster that is assigned to that phone.

What is an Activation Code?

An activation code is a single-use, 16-digit value that a user must enter on a phone before registering the phone. The user must enter the correct code, or the phone does not register. Activation codes provide a secure method to onboard phones without requiring an administrator to collect and input the MAC Address for each phone manually.

Custom Certificates (Optional)

If you want to use your own certificates, you can use the cloud to distribute certificates to MRA phones so that they can establish trust with Expressway. With this option, you must upload your certificates first to Expressway, and then to the **PhoneEdge-trust** store on Cisco Unified Communications Manager. The certificates are uploaded to the Cisco cloud so that the phone can download them during the device activation process.

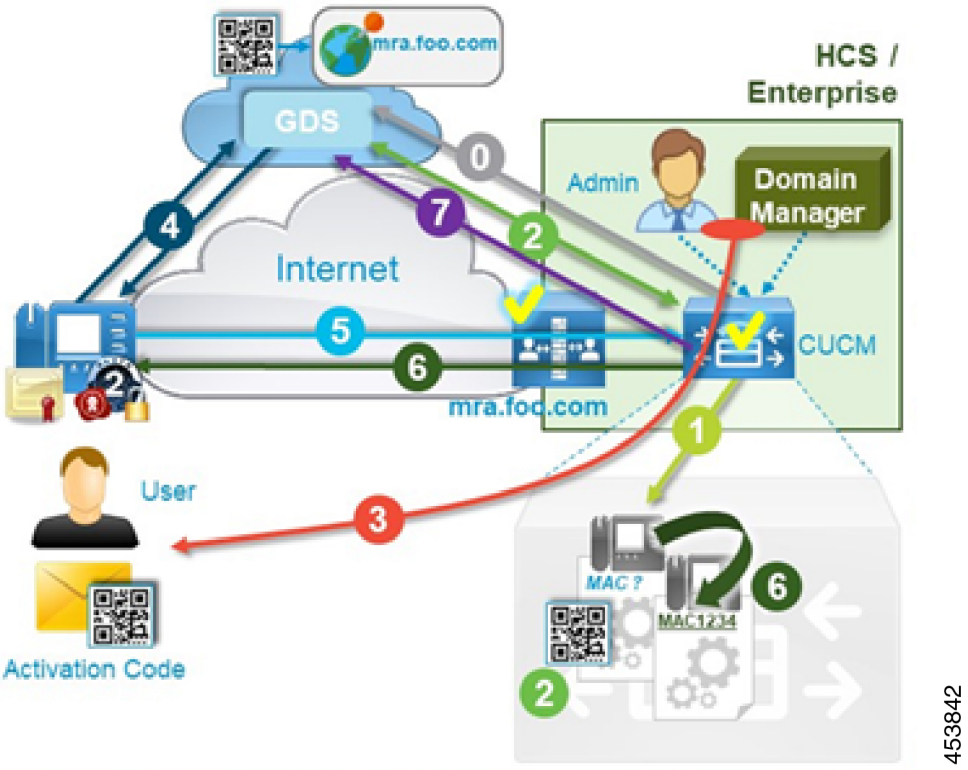
MRA Onboarding Process Flow

The below table contains the process flow for onboarding new MRA phones via Device Activation Code Onboarding in MRA mode. Match each numbered step to the subsequent graphic for an illustration of the process.

Note When you start Device Activation Service on UCM publisher to on-board clients over Mobile and Remote Access, you need to start the UDS and CCM services as well. Moreover, delete and rediscover the UCM cluster in Unified Communications configuration in Expressway-C, as doing a refresh of servers will not work.

Process Step	Process Flow
0	Administrator configures Cloud Onboarding and specifies the MRA Activation Domain and any MRA Service Domains.
1	Administrator provisions full device configuration without specifying the MAC address. The device name will be a random BAT MAC address.
2	Administrator requests activation code for this device. Device Activation Service requests the code from the cloud-based device activation service.
3	Activation Code is sent to the user (either via email or via the Self-Care Portal).
4	User enters the activation code. Phone gets the MRA target from the cloud.
5	Phone learns the location of Expressway and authenticates using the MIC + activation code in an SRP handshake.
6	Device activation service updates the device configuration in the database with the phone MAC and sends success to the phone
7	The phone can register and gets its phone specific configuration file from TFTP and then register with Unified CM. If the phone is assigned to a different MRA Service Domain, a redirect is provided in the configuration file. The phone can then register using the MRA Service Domain.
8	Device Activation Service releases the activation code from the cloud. The code can be reused in the future.

Figure 1: MRA Device Onboarding Process Flow with Activation Codes



Device Onboarding Prerequisites

The following table has support information for Activation Code Onboarding for MRA endpoints:

Table 1: MRA Activation Code Onboarding Support Information

Support	Details
Minimum Releases	Expressway X12.5.1 Cisco Unified Communications Manager 12.5(1)SU1 Cisco IP Phone firmware 12.5(1)SR3
Supported Endpoints	Cisco IP Phones 7811, 7821, 7832, 7841, 7861, 8811, 8832, 8832NR, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR

Note As of release X14.0, if you are onboarding supported Cisco IP Phone 78xx Series and 88xx Series phones for Mobile and Remote Access, the phones switch to MRA mode only if the **Allow Activation Code via MRA** checkbox is checked within the **Phone Configuration** window of **Cisco Unified Communications Manager**.

Using this approach, you must configure Activation Code onboarding for MRA phones. In addition, the MRA phone user must enter the correct activation code to activate and use the phone.

For details on configuring Activation Code Onboarding, see the "Device Onboarding via Activation Codes" chapter of *Feature Configuration Guide for Cisco Unified Communications Manager*.

In addition, the following prerequisites exist:

- If you've upgraded Expressway from a release prior to X12.5, refresh your Unified CM servers on Expressway-C before you configure this feature. On Expressway-C go to **Configuration** > **Unified Communications** > **Unified CM servers** and click **Refresh servers**.
- **Cisco Device Activation Service**—This service must be running on Cisco Unified Communications Manager (the service is running by default). Check the list of services in Cisco Unified Serviceability to verify the service is running.
- **OAuth Refresh Logins**—This feature must be enabled in Cisco Unified Communications Manager by setting the **OAuth Refresh Login Flow** enterprise parameter to **Enabled**.
- **Self-Care Portal**—If you want users to be able to use the Self-Care Portal to activate their phones:
  - The **Show Phones Ready to Activate** enterprise parameter must be set to **True** in Cisco Unified Communications Manager.
  - End users require login access to the portal. See the "Self-Care Portal" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager* for Self-Care configuration details.
  - The Self-Care Portal is not supported over MRA so remote users may need a VPN to access the portal.
- **DNS SRV records**—For the MRA Activation Domain and any MRA Service Domains, you must configure *_collab_edge* SRVs that point to the appropriate Expressway clusters.
- **TCP port 443 network requirement for the Cisco Cloud onboarding**—Connectivity must be enabled from Unified Communications Manager and IM and Presence Service/publisher over TCP port 443 for the following URLs/connections to the Cisco Cloud.
  - fos-a.wbx2.com
  - idbroker.webex.com
  - push.webexconnect.com
  - btpush.webexconnect.com

Note The TCP port 443 must be open from the Cisco Unified CM publisher node for outbound HTTPS requests (Cisco Cloud onboarding).

MRA Device Onboarding Configuration Flow

Follow these procedures to configure MRA Device Onboarding using activation codes in MRA mode.

Steps	Procedures
Step 1	Enable OAuth Authentication in Cisco Unified Communication Manager and Expressway: **1.** Enable OAuth on Cisco Unified CM: **a.** From Cisco Unified CM Administration, go to **System** > **Enterprise Parameters**. **b.** Set the **OAuth Refresh Login Flow** parameter to **Enabled**. **c.** Click **Save**. **2.** Enable OAuth Refresh authentication on Expressway: **a.** Go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**. **b.** Set **Authorize by OAuth token with refresh** to **On**. **c.** Click **Save**.
Step 2	Onboard Cisco Unified Communication Manager to the cloud for MRA activation code onboarding. **1.** From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**. **2.** Click the **Generate Voucher** button. **3.** Check the **Enable Activation Code Onboarding with Cisco Cloud** check box. **4.** Specify the **MRA Activation Domain**. **5.** Click **Save**. **Note** • Collab-edge DNS records must exist for the MRA Activation domain. • There is a limit of one MRA Activation Domain per cluster. The MRA Activation is added automatically to the list of MRA Service Domains.

Steps	Procedures
Step 3	Configure MRA Service Domains. **1.** From Cisco Unified CM Administration, choose **Advanced Features** > **MRA Service Domains**. **2.** If you have multiple Expressway clusters, add each domain where your MRA endpoints will operate. **3.** Check the **IsDefault** check box, if you want a domain to be applied as a clusterwide default MRA Service domain. **4.** Click **Save**.
Step 4	Optional. Assign an MRA Service Domain to an existing device pool. This lets you assign a specific Expressway cluster to all MRA devices that use the device pool. **1.** From Cisco Unified CM Administration, choose **System** > **Device Pool**. **2.** Click **Find** and select the appropriate device pool. **3.** From the **MRA Service Domain** drop-down, select the domain that you want to assign to devices that use this device pool. **4.** Click **Save**.
Step 5	Configure MRA Access Control to allow activation code onboarding: **1.** From Expressway-C, choose **Configuration** > **Unified Communications** > **Configuration**. **2.** Set **Authorize by OAuth token with refresh** to **On**. **3.** Set **Allow activation code onboarding** to **Yes**.
Step 6	Check Trusted Cisco Manufacturing Installed Certificates (MICs) installed. They are required to access the activation code onboarding functionality: **Note** Cisco Manufacturing Root certificates must be present in the *CallManager-trust* store to perform onboarding activity. **1.** On Expressway-E, choose **Maintenance** > **Security** > **Trusted CA certificate**. **2.** Click **Activation code onboarding trusted CA certificates**.
Step 7	Optional. If you want to use your own custom certificates. **1.** Upload the certificates to Expressway. **2.** Upload certificates to PhoneEdge-trust on Unified Communications Manager. Unified Communications Manager uploads the certificates to the cloud. During the activation process, the phone downloads the certificates from the cloud, thereby ensuring that the phone can communicate with Expressway.

Steps	Procedures
Step 8	Provision the phone in the Cisco Unified Communications Manager database using any accepted provisioning method. No matter which option you choose, make sure that both of the following check boxes are checked: • **Requires Activation Code Onboarding** • **Allow Activation Code via MRA** **Note** You can provision the phone with a dummy MAC address. The onboarding process updates the **Device Name** using the phone's actual MAC address. For sample provisioning procedures using either the GUI or Bulk Administration, see the "Device Onboarding via Activation Codes" chapter of the *System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1* or later.
Step 9	Ship the phone to the MRA users.

Activate Phones

Administrators have two options for sending activation codes to phone users:

- Self-Care Portal—Phone users can log in to the portal to view their phone's activation code and an accompanying barcode. They can either key the activation code onto the phone or use the phone's video camera to scan the barcode—both methods work. Review Device Onboarding Prerequisites for information about Self-Care requirements.
- CSV File Export—In Cisco Unified Communications Manager, administrators can export a csv file of outstanding activation codes and associated users. They can use the contents of this file to notify MRA users with their activation codes. To export a csv file:
  1. From Cisco Unified CM Administration, choose **Device** > **Phone**.
  2. From **Related Links**, select **Export Activation Codes** and click **Go**.

Note Activation Codes have a default lifetime of 168 hours (7 days). You can reconfigure this value via the **Activation Time to Live (Hours)** service parameter in Cisco Unified Communications Manager. If the activation code expires, the administrator can click **Release Activation Code** and then **Generate New Activation Code** from the **Phone Configuration** window in order to reset the activation code.

Entering the Activation Codes

When an MRA user plugs in their phone, they are prompted to enter the activation code. Once they enter the activation code, or scan the barcode that displays in Self-Care, the phone onboards, downloads its configuration file, and registers.

The phone is now ready to use.

Additional Options for Secure Onboarding

The following options slightly modify the configuration process for added security:

Option 1: Administrator provisions phone with actual MAC address

Rather than using a dummy MAC address, the administrator adds the phone to Cisco Unified Communications Manager with the actual MAC address. This method ties the activation code to the actual phone MAC address, enhancing security as the activation code works on that phone only. However, this method requires that the administrator collect and enter each phone MAC address individually.

Option 2: Administrator activates phone on-Premises before sending to Remote User for reonboarding in MRA mode

With this method, the administrator activates the phone in on-premises mode before resetting the activation code requirement and shipping to the MRA user, who will activate the phone in MRA mode.

- Administrator configures Activation Code Onboarding (On-Premises mode) and provisions the phone with a dummy MAC address.
- Administrator onboards and registers the phone in the on-premises environment. This process updates the **Device Name** in Cisco Unified Communications Manager with the actual phone MAC address and lets the phone updates its firmware load.
- The administrator configures Activation Code Onboarding for MRA mode, resets the activation code requirement thereby locking the phone until the new code is entered.

Note In the **Phone Configuration** window, both of the following check boxes must be checked as they reset the activation code and lock the phone:

- **Requires Activation Code Onboarding**
- **Allow Activation Code via MRA**

- The administrator ships the phone to the MRA user and provides the user with the new activation code.
- The remote MRA user must enter the new activation code in order to use the phone.

This option provides the following benefits:

- Improves security as the activation code is tied to the MAC address and works for that phone only.
- Ensures that phone firmware is already up to date when the user receives the phone.
- Does not require the administrator to collect and input individual MAC addresses.

For information on how to configure activation code onboarding in On-Premises mode, see the On-Premises tasks in the “Device Onboarding via Activation Codes” chapter of the *System Configuration Guide for Cisco Unified Communications Manager.*