SIP OAuth Mode

SIP OAuth Mode Overview

Secure registrations to Unified Communications Manager involves a process of updating CTL files, setting up a mutual certificate trust store and so on. If devices are switching between on-premises and off-premises, it is difficult to update LSCs and renew Certificate Authority Proxy Function (CAPF) enrolment each time when a secure registration is completed.

SIP OAuth mode allows you to use OAuth refresh tokens for all devices authentication in secure environments. This feature enhances the security ofUnified Communications Manager.

Unified Communications Manager verifies the token presented by the endpoints and serves the configuration files only to authorized ones. OAuth token validation during SIP registration is completed when OAuth based authorization is enabled on Unified Communications Manager cluster and other Cisco devices.

OAuth support for SIP registrations is extended for

- Cisco Jabber devices from Cisco Unified Communications Manager 12.5 release onwards
- SIP Phones from Cisco Unified Communications ManagerRelease 14 onwards

Note By default, TFTP is secure for SIP phones when SIP OAUth is enabled. TFTP file download happens through secured channel, and only for authenticated phones. SIP OAuth provides end to end secure signaling and media encryption without CAPF on-premises as well as over MRA.

The following are the Phone Security Profile Types that can be configured for OAuth.

- Cisco Dual Mode For iPhone (TCT device)
- Cisco Dual Mode For Android (BOT device)
- Cisco Unified Client Service Framework (CSF device)
- Cisco Jabber for Tablet (TAB device)

- Universal Device Template
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 8832NR

SIP OAuth Mode Prerequisites

This feature assumes that you have already completed the following:

- Ensure Mobile and Remote Access is configured and the connection is established between Unified Communication Manager and Expressway.
- Ensure Unified Communications Manager is registered to a Smart or Virtual account with **allow export-controlled** functionality.
- Ensure client firmware supports SIP OAuth.

SIP OAuth Mode Configuration Task Flow

Complete the following tasks to configure SIP OAuth for your system.

Procedure

	Command or Action	Purpose
Step 1	Upload CA Certificate to the Phone Edge Trust	Upload CA Certificate to the phone edge trust to get the tokens. This step is not applicable for Cisco Jabber device.

	Command or Action	Purpose
Step 2	Enable OAuth Access Token for Devices	**Important** This step is applicable from Release 14 onwards. Enable OAuth for SIP registrations in Cisco IP Phone 7800 and 8800 enterprise series. This step is not applicable for Cisco Jabber device.
Step 3	Configure Refresh Logins, on page 4	Enable oauth with refresh login flow on Unified Communications Manager to register the device via SIP OAuth.
Step 4	Configure OAuth Ports, on page 5	Assign the ports for OAuth for each node that has OAuth registration.
Step 5	Configure OAuth Connection to Expressway-C, on page 5	Configure a mutually authenticated TLS connection to Expressway-C.
Step 6	Enable SIP OAuth Mode, on page 6	Enable OAuth services using a CLI command on the publisher node.
Step 7	Restart Cisco CallManager Service, on page 6	Restart this service on all nodes that have OAuth registrations.
Step 8	Configure Device Security Mode in Phone Security Profile	Configure OAuth support within a Phone Security Profile if you are deploying encryption for the endpoints.
Step 9	(Optional) Configure SIP Oauth Registered Phones for MRA Mode	**Important** This step is applicable from Release 14 onwards. Configure SIP OAuth registered phones in MRA mode. This step is not applicable for Cisco Jabber device.

Upload CA Certificate to the Phone Edge Trust

Use this procedure to upload the root certificate of Tomcat signed certificate to the Phone Edge Trust.

Note This procedure is performed only for Cisco Phones and not applicable for Cisco Jabber.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 In the **Upload Certificate/Certificate chain** window, from the **Certificate Purpose** drop-down list choose **Phone-Edge-Trust**.

Step 4 In the **Upload File** field, click **Browse** and upload the certificate.

Step 5 Click **Upload**.

Enable OAuth Access Token for Devices

Important This section is applicable from Release 14 onwards.

Use this procedure to enable OAuth access token for phones.

Note Configure this enterprise parameter only for OAuth support for SIP registrations for phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **SSO and OAuth Configuration** section, ensure that the value of **OAuth Access Token for Devices** drop-down list is set to **Implicit:Already registered devices**.

Note Set the value of **OAuth Access Token for Devices** to **Explicit:Activation Code device onboarding required** to disable implicitly receiving tokens for SIP OAuth registration and only support receiving tokens through activation code. The tokens can then be used for SIP OAuth registration if indicated in the security profile.

From Release 14 onwards, the default value of the enterprise parameter **OAuth Access Token for Devices** is **Implicit:Already registered devices**.

Step 3 Click **Save**.

Configure Refresh Logins

Use this procedure to configure Refresh Logins with OAuth access tokens and refresh tokens for Cisco Jabber clients.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **SSO and OAuth Configuration**, set the **OAuth with Refresh Login Flow** parameter to **Enabled**.

Step 3 (Optional) Set any other parameters in the **SSO and OAuth Configuration** section. For parameter descriptions, click on the parameter name.

Step 4 Click **Save**.

Configure OAuth Ports

Use this procedure to assign the ports that are used for SIP OAuth.

Procedure

Step 1 From Cisco Unified CM Administration, choose, **System** > **Cisco Unified CM**.

Step 2 Do the following for each server that uses SIP OAuth.

Step 3 Select the server.

Step 4 Under Cisco Unified Communications Manager **TCP Port Settings**, set the port values for the following fields:

- SIP Phone OAuth Port

  Default value is 5090. Acceptable configurable range is 1024–49151.

- SIP Mobile and Remote Access Port

  Default value is 5091. Acceptable configurable range is 1024–49151.

Note Cisco Unified Communications Manager uses SIP Phone OAuth Port (5090) to listen for SIP line registration from Jabber on-premises devices over TLS. However, Unified CM uses SIP Mobile Remote Access Port (default 5091) to listen for SIP line registrations from Jabber over Expressway through mTLS.

Both ports use the Cisco Tomcat certificate and Tomcat-trust for incoming TLS/mTLS connections. Make sure that your Tomcat-trust store is able to verify the Expressway-C certificate for SIP OAuth mode for Mobile and Remote Access to function accurately.

You must perform extra steps to upload the Expressway-C certificate into the Tomcat-Trust certificate store of the Cisco Unified Communications Manager, when:

- Expressway-C certificate and Cisco Tomcat certificate is not signed by the same CA certificate.
- Unified CM Cisco Tomcat certificate is not CA signed.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each server that uses SIP OAuth.

Configure OAuth Connection to Expressway-C

Use this procedure to add the Expressway-C connection to Cisco Unified Communications Manager Administration. You need this configuration for devices in Mobile and Remote Access mode with SIP OAuth.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Expressway-C**.

Step 2 (Optional) In the **Find and List Expressway-C** window, click **Find** to verify X.509 Subject Name/Subject Alternate Name that is pushed from the Expressway-C to Unified Communications Manager.

Note If required, you can modify the values. Alternatively, if the entries are missing, add Expressway-C information.

If the Expressway-C has a different domain than the Unified Communications Manager, then the administrator needs to access the Cisco Unified CM Administration User Interface and add the domain to the Expressway C in the Unified CM configuration.

Step 3 Click **Add New**.

Step 4 Enter an IP Address, Hostname or fully qualified domain name for the Expressway-C.

Step 5 Enter a Description.

Step 6 Enter the X.509 Subject Name/Subject Alternate Name of the Expressway-C from the Expressway-C certificate.

Step 7 Click **Save**.

Enable SIP OAuth Mode

Use the Command Line Interface to enable SIP OAuth mode. Enabling this feature on the publisher node also enables the feature on all cluster nodes.

Before you begin

From Release 14SU1 onwards, when Proxy TFTP is enabled, you should copy the root CA certificate for the off-cluster Tomcat certificate to the proxy phone edge trust.

Procedure

Step 1 On the Unified Communications Manager publisher node, log in to the Command Line Interface.

Step 2 Run the `utils sipOAuth-mode enable` CLI command.
From Release 14 onwards, the system updates the read-only **Cluster SIPOAuth Mode** enterprise parameter to **Enabled**.

Restart Cisco CallManager Service

After enabling SIP OAuth through CLI, restart the Cisco CallManager service on all nodes where endpoints register through SIP OAuth.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center** > **Feature Services**.

Step 2 From the **Server** drop-down list, select the server.

Step 3 Check the **Cisco CallManager** service and click **Restart**.

Configure Device Security Mode in Phone Security Profile

Use this procedure to configure the device security mode in the phone security profile and is required only if you have set the **Device Security Mode** within that phone's **Phone Security Profile** to **Encrypted**.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform either of the following:

- Search for an existing phone security profile
- Click **Add New**

Step 3 In the Phone Security Profile Information section, from the **Device Security Mode** drop-down list, choose **Encrypted**.

Step 4 From the **Transport Type** drop-down list, choose **TLS**.

Step 5 Check the **Enable OAuth Authentication** check box.

Step 6 Click **Save**.

Step 7 Associate the Phone Security Profile to the phone. For more information on how to apply the phone security phones, see "Apply Security Profiles to Phone" section in Security Guide for Cisco Unified Communications Manager.

Note Reset your phone for the changes to take effect.

Note When SIP OAuth Mode is enabled, **Enable Digest Authentication** and **TFTP Encrypted Config** options are not supported. Phones will download the TFTP config file securely over **https(6971)** and use the token for authentication.

Configure SIP Oauth Registered Phones for MRA Mode

Use this procedure to configure SIP OAuth registered phones to MRA mode.

Before you begin

Important This section is applicable from Release 14 onwards.

Make sure your phones are configured to use Activation Codes. For more information see *Set Registration Method to use Activation Codes* section in System Configuration Guide for Cisco Unified Communications Manager.

Note When using SIP OAuth over MRA , user cannot use username / password for login but have to use activation code based onboarding

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the device which you want to configure for off-premises mode.

Step 3 In the **Device Information** section, do the following:

- Check **Allow Activation Code via MRA** check box.
- From the **Activation Code MRA Service Domain** drop-down list, choose the required MRA service domain. For more information on how to configure the MRA service domain see, the *MRA Service Domain Configuration* section in System Configuration Guide for Cisco Unified Communications Manager.

Note For SIP OAuth over MRA mode, use only activation code and do not use username/password based login.

Step 4 In the **Protocol Specific Information** section, choose the OAuth enabled SIP profile from the **Device Security Profile** drop-down list. Make sure that the phone supports OAuth firmware. For more information, on how to create a security profile, see *Configure Phone Security Profile* section in System Configuration Guide for Cisco Unified Communications Manager.

Step 5 Click **Save** and **Apply Configuration**.

Note The phone switches to MRA mode and initiates communication with the Expressway. If your internal network does not allow communication with Expressway from on-premises, the phone doesn't register but is ready to contact Expressway when it's powered up off-premises.