



Digest Authentication Setup for SIP Trunks

This chapter provides information about digest authentication setup for SIP trunks. When you configure digest authentication for SIP trunks, Unified Communications Manager challenges the identity of the SIP user agent when it receives a SIP request on the SIP trunk. The SIP user agent, in turn, can challenge the identity of Unified Communications Manager when Unified Communications Manager sends a SIP request to the trunk. For additional information on how digest authentication works for SIP trunks, see [Digest Authentication](#).

- [Set Up SIP Trunk Digest Authentication, on page 1](#)
- [Set Up Digest Authentication Enterprise Parameters, on page 2](#)
- [Set Up Digest Credentials, on page 2](#)
- [Application User Digest Credential Settings, on page 2](#)
- [Find SIP Realm, on page 3](#)
- [Configure SIP Realm, on page 3](#)
- [SIP Realm Settings, on page 4](#)
- [Delete SIP Realm, on page 4](#)

Set Up SIP Trunk Digest Authentication

The following procedure describes the tasks to configure digest authentication for SIP trunks.

Procedure

- Step 1** Configure the SIP trunk security profiles; make sure that you check the **Enable Digest Authentication** check box.
- Step 2** Apply a SIP trunk security profile to the trunk.
- Step 3** Configure the enterprise parameter, Cluster ID, if not configured.
- This parameter supports Unified Communications Manager challenges to the identity of the SIP user agent that is sending a SIP request on the SIP trunk.
- Step 4** If Unified Communications Manager challenges the identity of SIP user agents that are sending SIP requests on the SIP trunk, configure the digest credentials for the application user in the **Application User Configuration** window.
- Step 5** If Unified Communications Manager responds to challenges from a trunk peer, configure the SIP realm.
-

Set Up Digest Authentication Enterprise Parameters

To configure the enterprise parameter, Cluster ID, for digest authentication, choose **System > Enterprise Parameters** in Unified Communications Manager Administration. Locate the Cluster ID parameter and update the value, as described in the Help for the parameter. This parameter supports Unified Communications Manager challenges to the identity of the SIP user agent that is sending a SIP request on the SIP trunk.



Tip To access the Help for the parameter, click the question mark that displays in the **Enterprise Parameters Configuration** window or click the parameter link.

Set Up Digest Credentials

If Unified Communications Manager challenges the identity of a SIP user agent, you must configure the digest credentials for the application user in the Application User Configuration window in Unified Communications Manager Administration. Unified Communications Manager uses these credentials to verify the identity of SIP user agents that are sending requests through the SIP trunk.

To configure the digest credentials for an application user, perform the following procedure:

Procedure

- Step 1** Find the application user, as described in the *Administration Guide for Cisco Unified Communications Manager*.
- Step 2** Click the application user link.
- Step 3** After the specific **Application User Configuration** window displays, enter the appropriate settings, as described in [Table 2: SIP Realm Security Profile, on page 4](#).
- Step 4** Click **Save**.

Application User Digest Credential Settings

The following table describes the settings for the digest credential settings in the **Application User Configuration** window in Unified Communications Manager Administration.

Table 1: Digest Authentication Credentials

Setting	Description
Digest Credentials	Enter a string of alphanumeric characters.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.

Find SIP Realm

To find a SIP Realm, perform the following procedure:

Procedure

- Step 1** In Unified Communications Manager Administration, choose **User Management > SIP Realm**.
The **Find and List** window displays. Records from an active (prior) query may also display in the window.
- Step 2** To find all records in the database, ensure the dialog box is empty; go to [Step 3, on page 3](#).
To filter or search records
- From the first drop-down list box, choose a search parameter.
 - From the second drop-down list box, choose a search pattern.
 - Specify the appropriate search text, if applicable.
- Note** To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.
- Step 3** Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the **Rows per Page** drop-down list box.
- Step 4** From the list of records that display, click the link for the record that you want to view.
- Note** To reverse the sort order, click the up or down arrow, if available, in the list header.
The window displays the item that you choose.
-

What to do next

If you have not already done so, configure the Cluster ID enterprise parameter.

Configure SIP Realm

If Unified Communications Manager responds to challenges from one or more trunk peers, you must configure SIP Realm for each SIP trunk user agent that can challenge Unified Communications Manager.

To add or update a SIP Realm, perform the following procedure:

Procedure

- Step 1** In Unified Communications Manager Administration, choose **User Management > SIP Realm**.
- Step 2** Enter the appropriate settings as described in [Table 2: SIP Realm Security Profile, on page 4](#).
- Step 3** Click **Save**.
- Step 4** Perform the procedure for all realms that you must add or update.
-

What to do next

To ensure that digest authentication is successful, verify that the same settings that you configured in Unified Communications Manager are configured on the SIP user agent.

SIP Realm Settings

The SIP Realm provides the trunk-side credentials when Unified Communications Manager gets challenged by a trunk peer.

The following table describes the settings for the SIP Realm.

Table 2: SIP Realm Security Profile

Setting	Description
Realm	Enter the domain name for the realm that connects to the SIP trunk; for example, SIPProxy1_xyz.com. You can use alphanumeric characters, period, dash, underscore, and space.
User	Enter the user name for the SIP user agent in this realm; for example, enter the Unified Communications Manager server name. The SIP trunk uses this user name to challenge this Unified Communications Manager.
Digest Credentials	Enter the password that Unified Communications Manager uses to respond to a challenge for this realm and user.
Confirm Digest Credentials	Re-enter the password for verification.

Delete SIP Realm

This section describes how to delete a SIP Realm from the Unified Communications Manager database.

Procedure

- Step 1** Find the SIP Realm to delete.
- Step 2** Perform one of the following tasks:
- To delete multiple SIP Realms, perform one of these tasks in the **Find and List** window:

- Check the check boxes next to the realms that you want to delete; then, click **Delete Selected**.

You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

b) To delete a single SIP Realm, perform one of these tasks in the **Find and List** window:

- Check the check box next to the realm that you want to delete; then, click **Delete Selected**.

Click the **Name** link for the realm. After the specific **SIP Realm Configuration** window displays, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.
