# Digest Authentication for SIP Phones Setup

This chapter provides information about digest authentication for SIP phones setup. For additional information on how digest authentication works for phones that are running SIP, see Digest Authentication.

When you enable digest authentication for a phone, Unified Communications Manager challenges all requests except keepalive messages for phones that are running SIP. Unified Communications Manager uses the digest credentials for the end user, as configured in the **End User Configuration** window, to validate the credentials that the phone offers.

If the phone supports extension mobility, Unified Communications Manager uses the digest credentials for the extension mobility end user, as configured in the **End User Configuration** window, when the extension mobility user logs in.

For information about configuring digest authentication for non-Cisco phones that are running SIP, refer to Appendix C in the *Administration Guide for Cisco Unified Communications Manager*.

# Enable Digest Authentication in Phone Security Profile

Use this procedure to enable digest authentication for a phone through the Phone Security Profile.

**Procedure**

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

**Step 2**     Click **Find** and choose the phone security profile that is associated to the phone.

**Step 3**     Check the **Enable Digest Authentication** check box.

**Step 4**     Click **Save**.

# Configure SIP Station Realm

Assign the string that Cisco Unified Communications Manager uses in the Realm field when challenging a SIP phone in the response to a 401 Unauthorized message. This applies when the phone is configured for digest authentication.

✎

**Note**    The default string for this service parameter is ccmsipline.

**Procedure**

**Step 1**    From Unified Communications Manager, choose **System** > **Service Parameters**.

**Step 2**    From the **Server** drop-down list, choose a node where you activated the CiscoCallManager service.

**Step 3**    From the **Service** drop-down list, choose the CiscoCallManager service. Verify that the word "Active" displays next to the service name.

**Step 4**    Update the **SIP Realm Station** parameter, as described in the help. To display help for the parameters, click the question mark or the parameter name link.

**Step 5**    Click **Save**.

# Assign Digest Credentials to Phone User

Use this procedure to assign digest credentials to the end user who owns the phone. Phones use the credentials to authenticate.

**Procedure**

**Step 1**    From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

**Step 2**    Click **Find** and choose the end user who owns the phone.

**Step 3**    Enter the credentials in the following fields:

- Digest Credentials

- Confirm Digest Credentials

**Step 4**    Click **Save**.

# End User Digest Credential Settings

To view the digest credentials details, perform the following procedure:

From Cisco Unified Communications Manager Administration, choose **User Management > End User** and click the User ID and the **End User Configuration** window appears. The digest credentials are available in the **User Information** pane of the **End User Configuration** window.

*Table 1: Digest 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. |

# Assign Digest Authentication to the Phone

Use this procedure to associate the digest user and digest authentication-enabled security profile to the phone.

**Procedure**

| | |
|---|---|
| **Step 1** | From Cisco Unified Communications Manager Administration, choose **Device > Phone**. |
| **Step 2** | Click **Find** and choose the phone for which you want to assign digest authentication. |
| **Step 3** | From the **Digest User** drop-down list, assign the end user for whom you assigned digest credentials. |
| **Step 4** | Make sure that the phone security profile for which you enabled digest authentication is assigned through the **Device Security Profile** drop-down list. |
| **Step 5** | Click **Save**. |
| **Step 6** | Click **Reset**. |

After you associate the end user with the phone, save the configuration and reset the phone.