



Self Care Portal

- [Self Care Portal Overview, on page 1](#)
- [Self Care Portal Task Flow, on page 1](#)
- [Self Care Portal Interactions and Restrictions, on page 3](#)

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize features and settings for their phones. As the administrator, you control access to the portal. Before an end user can access the portal, you must add the user to the default **Standard CCM End Users** access control group, or to any access control group that has the **Standard CCM End Users** role assignment. In addition, users require their user ID, password, and the URL with which to access the portal. Users can access the portal via the following URL:

```
http(s)://<server_name>:<port_number>/ucmuser/
```

where:

- **<server_name>** represents the Unified Communications Manager IP address, hostname or fully qualified domain name
- **<port_number>** represents the port on which to connect. The port is optional, but is useful in firewall situations.
- **ucmuser** is a mandatory subpath that points to Self Care

Optionally, you can also configure enterprise parameters within Cisco Unified Communications Manager in order to assign which phone settings are available for end users to configure. For example, the **Show Call Forwarding** enterprise parameter determines whether users can configure Call Forward via the portal.

Self Care Portal Task Flow

Procedure

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | Grant User Access to the Self Care Portal, on page 2 | To access the portal, end users must be assigned to the Standard CCM End Users access |

| | Command or Action | Purpose |
|---------------|---|---|
| | | control group or to any group that has the Standard CCM End Users role assignment. |
| Step 2 | Configure the Self Care Portal Options, on page 2 | Configure enterprise parameters in order to control what configuration options are available to users whom access the portal. |

Grant User Access to the Self Care Portal

To access the portal, end users must be assigned to the **Standard CCM End Users** access control group or to any group that has the **Standard CCM End Users** role assignment.

Procedure

-
- Step 1** From Cisco Unified CM Administration, choose **User Management > End User**.
- Step 2** Search for the user for whom you want to provide Self-Care access.
- Step 3** In the **End User** section, ensure that the user has a password and PIN configured.
Usually these credentials are entered when a new user is added.
- Step 4** In the **Permission Information** section, click **Add to Access Control Group**.
- Step 5** Click **Find** and select the **Standard CCM End Users** group or a customized group that contains the **Standard CCM End Users** role.
- Note** For information on how to edit access control groups, and role assignments for access control groups, refer to the "Manage User Access" chapter of the *Administration Guide for Cisco Unified Communications Manager*.
- Step 6** Select **Save**.
-

Configure the Self Care Portal Options

Use this procedure to configure Self Care Portal enterprise parameters in order to control what configuration options are available to users whom access the portal.

Before you begin

[Grant User Access to the Self Care Portal, on page 2](#)

Procedure

-
- Step 1** From Cisco Unified Communications Manager Administration, select **System > Enterprise Parameters**.
- Step 2** Under **Self Care Portal Parameters**, set the **Self Care Portal Default Server** by selecting one of the available servers from the drop-down list.

This parameter determines which Cisco Unified CM server Jabber uses to display embedded Self Care options pages. If you select **None**, Jabber defaults to the Publisher.

- Step 3** Configure any of the remaining Self Care Portal Parameters to enable or disable features for the portal. For help with the fields, refer to the enterprise parameters help.
- Step 4** Select **Save**.

Self Care Portal Interactions and Restrictions

The following table highlights feature interactions and restrictions with the Self-Care Portal.

| Feature | Interaction or Restriction |
|--|---|
| Device Onboarding via Activation Codes | <p>If you want users to be able to activate their phones via the Self-Care Portal, the Show Phones Ready to Activate enterprise parameter must be set to True (this is the default setting).</p> <p>With this feature, users can obtain their activation code by logging in to the Self-Care portal. They can either use the phone's video camera to scan the barcode, or they can enter the code manually on the phone in order to activate and register the phone.</p> <p>For more information on activation codes, see the "Device Onboarding via Activation Codes" chapter of the <i>System Configuration Guide for Cisco Unified Communications Manager</i>.</p> |
| Authenticated user https request | <p>When an authenticated user makes a request to <code>https://{CUCM_address}/ucmuser/hostAlive/{host}</code>, the following happens:</p> <ul style="list-style-type: none"> • If the request is successful at getting <code>http://{host}/</code> or if the request can ping <code>{host}</code> Cisco Unified Communications Manager returns the string, <code>"true"</code>. • If the request is unsuccessful, Cisco Unified Communications Manager returns the string <code>"false"</code>. |
| Maximum Login for Extension Mobility | <p>For end users to be able to configure this setting within the Self-Care Portal, an administrator must have checked the Allow End User to set their Extension Mobility maximum login time option in the associated User Profile of Cisco Unified CM Administration.</p> <p>If this option is selected within the User Profile, for all users whom use the profile, the Self-Care Portal setting overrides the administrator-configured values of the Intra-cluster Maximum Login Time and Inter-cluster and Maximum Login Time service parameters in Cisco Unified Communications Manager.</p> |

