# Introduction

## User Interface

You can use a variety of browsers to access the Self Service interface. For a list of browsers, refer to *Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide*.

**Note** Obtain the address (URL) of your Self Service web pages, your username, and your password from your System Administrator.

Use this procedure to log in to the Self Service interface.

### Procedure

**Step 1** Enter *https://<service-ip-or-node-name>/selfservice/#/login?theme=cisco_selfservice&lang=<language>* in your browser URL field; for example https://172.29.21.200/selfservice/#/login?theme=cisco_selfservice&lang=en-us. With this example, the Self Service interface uses the Cisco selfservice theme and the text on the Login page is displayed in English.

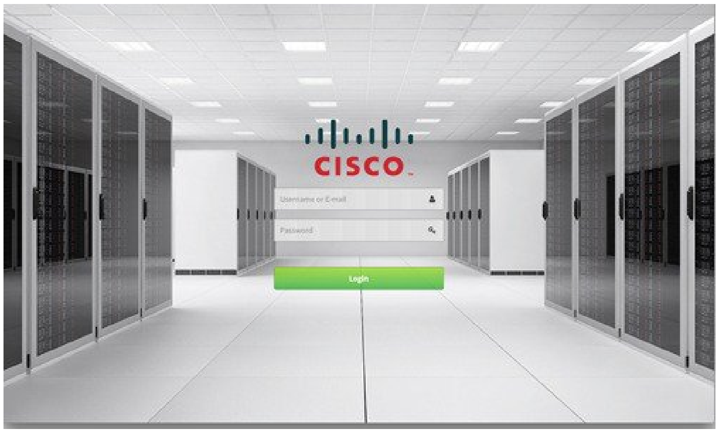
**Step 2** Enter your username or email address.

**Note** You can also log in with a username such as cisco-sub@sys.p1.r1.c1.s1, although most users log in using their email address.

**Step 3** Enter the password provided by your administrator.

**Step 4** Click **Login.**

*Figure 1: Login Screen*

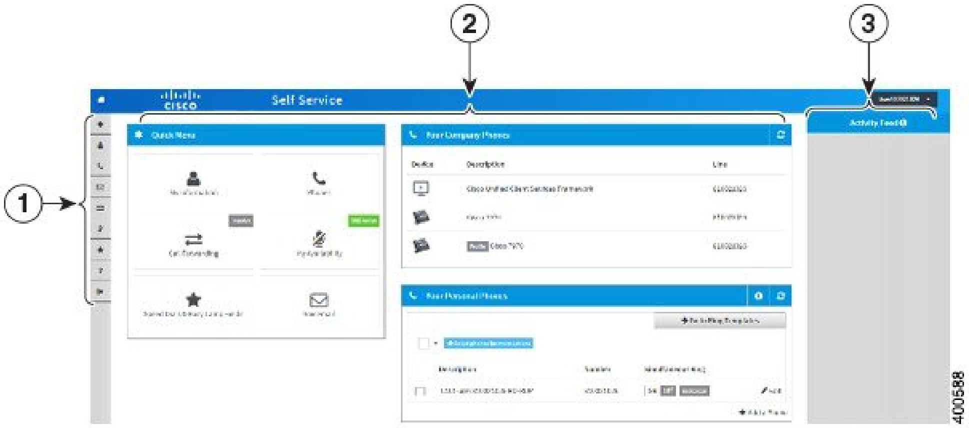


By default, when you log in to the Self Service interface, the landing page appears. The landing page cannot be customized in this release of the user interface. For more information on the user roles and themes that are available, refer to *Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide*.

If you are logging in for the first time, you may be prompted to change your password. See First Login, on page 3.

The Landing Page consists of three main areas as shown in the following figure:

*Figure 2: Landing Page*



1 **Button Bar**—This bar is located on the left-hand side of the screen. The buttons provide links to the various functions in Self Service. Refer to Buttons and Icons and Common Tasks for a description of all buttons on the button bar, as well as miscellaneous buttons and icons used in Self Service.

2 **Dashboard**—This is the center, main area of the screen. It provides quick links to the main Self Service functionality, as well as a summary view of your company phones (as configured by your Administrator) and personal phones that you configured yourself.

3 **Activity Feed Area**—This is located on the right-hand side of the screen. This area displays an activity log of all activities that occurred in the current browser session. Directly above the Activity Feed area, the currently logged in user is displayed. There are four options available from this dropdown list:

- **My Information**—Also accessed from the Button Bar. See My Information for details.
- **Help**—Also accessed from the Button Bar. See My Information for details.
- **Password Reset Questions**—Allows you to configure your password reset questions. See Configure Your Password Reset Questions for details.
- **Logout**—Also accessed from the Button Bar. See My Information for details.

# First Login

If configured by your Administrator, you may be prompted to change your password when you login to Self Service for the first time.

**Note** First login password change applies only to Cisco Unified Communications Domain Manager 10.6(1) authenticated users. It does not apply to SSO or LDAP authenticated users.

### Procedure

**Step 1** Enter the current password in the Current Password field.
**Step 2** Enter the new password in the New Password field.
**Step 3** Re-enter the new password in the Confirm New Password field.
**Step 4** Click the **Change** button.
**Step 5** Browse to the website address provided using a web browser.

# Password Hints and Rules

When considering a password, make sure that it complies with the following:

- Must consist of at least eight characters, and contain at least:

- ◦ one uppercase letter
- ◦ one lowercase letter
- ◦ one number
- ◦ one symbol. Supported symbols are ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ { ] } | : ; ‘ ” , < . > / and ?

- Do not use keyboard patterns based or obvious passwords such as a birthday or your name.
- Do not share your passwords with other users.
- Do not write down your password or store it in an obvious place, such as on a pin-board or in a diary.

# Session Timeout

To assist in data security, Self Service has been designed with an automatic session timeout feature. Session timeouts are configured in your credential policy by your administrator.

**Note** Session timeouts do not apply to SSO authenticated users.

The main reason for this is that Cisco Unified Communications Domain Manager 10.6(1) could prematurely expire a session before the IDP has expired, resulting in a false sense of security on Cisco Unified Communications Domain Manager 10.6(1) while the IDP session is still alive.

Cisco Unified Communications Domain Manager 10.6(1) honors the the SessionNotOnOrAfter SAML 2.0 attribute. This is equivalent to an absolute session timeout, although controlled by the IDP.

There are two types of timeouts:

**Idle Timeout**

Defines the number of minutes a session remains active when there is no activity in the session. Default is 20 minutes.

**Absolute Timeout**

Defines the maximum number of minutes a session can be active. Default is 1440 minutes (24 hrs).

In both instances, the following message is displayed to notify you of a pending timeout:

```
Your session will expire in 30 seconds
```

### Idle Timeout

Any mouse or keyboard activity after receiving session timeout notification is deemed as 'activity' and results in the extension of your current session. If there is no activity within the specified time, you are automatically logged out of Self Service and returned to the Login screen, as soon as you try to perform a transaction.

### Absolute Timeout

After the time period elapses, you are automatically logged out of Self Service and returned to the Login screen.