



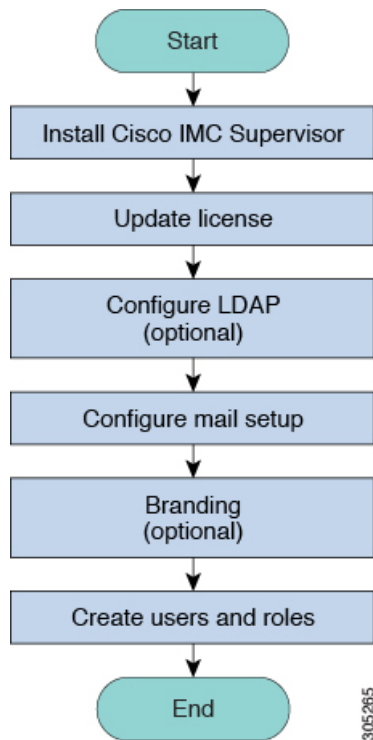
Getting Started

This chapter contains the following topics:

- [Overview, page 1](#)
- [Launching Cisco IMC Supervisor, page 2](#)
- [Licensing Tasks, page 3](#)
- [Authentication and LDAP Integration, page 4](#)
- [Configuring LDAP, page 5](#)
- [Configuring a SCP User, page 16](#)
- [Configuring Mail Setup, page 16](#)
- [Branding, page 17](#)
- [Configuring User Interface Settings, page 18](#)

Overview

The following figure illustrates the workflow to setup your environment using Cisco IMC Supervisor:



Launching Cisco IMC Supervisor

Cisco IMC Supervisor should have been successfully installed, with a correctly configured IP address.

Before You Begin

- Verify if Cisco IMC Supervisor is installed successfully.
- Ensure you have the IP address configured during the Cisco IMC Supervisor installation.

Procedure

Type the Cisco IMC Supervisor IP address in any browser URL and log in with the following credentials:

- User Name - admin
- Password - admin

Once you have logged in, Cisco IMC Supervisor will launch. You will see the default dashboard view of Cisco IMC Supervisor.

Licensing Tasks

You can use the License menu to view the license details and the usage of resources. The following licensing procedures are available from **Administration > License** menu.

Tab	Description
License Keys	This tab displays the details of the license used in Cisco IMC Supervisor. You can also use this tab to upgrade the license. You can upgrade the license when a new version of Cisco IMC Supervisor is available,
License Utilization	This tab shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page.
Resource Usage Data	This tabs displays the details of the various resources used.

Updating the License

You must perform the following procedure to update the license before you start using Cisco IMC Supervisor. For the list of valid licenses, see [About Licenses](#). You must generate a license key, claim and register the Product Access Key. After installing Cisco IMC Supervisor, the license is validated and you can start using Cisco IMC Supervisor.

Before You Begin

If you received a zipped license file by email, extract and save the **.lic** file to your local machine.

Procedure

-
- Step 1** From the menu bar, choose **Administration > License**.
 - Step 2** Select the **License Keys** tab.
 - Step 3** Click **Update License**.
 - Step 4** In the **Update License** dialog box, do one of the following:
 - To upload a **.lic** file, click **Browse**, navigate to and select the **.lic** file, then click **Upload**.
 - For a license key, check the **Enter License Text** check box then copy and paste the license key only into the **License Text** field. The license key is typically at the top of the file, after Key ->.

You can also copy and paste the full text of a license file into the **License Text** field.
 - Step 5** Click **Submit**.
The license file is processed, and a message appears confirming the successful update.
-

Running License Audit

Perform this procedure when you want run license audits.

Before You Begin

The license should be updated. To upgrade the license, refer [Updating the License](#), on page 3.

Procedure

-
- Step 1** From the menu bar, choose **Administration > License**.
 - Step 2** Click the **License Utilization** tab.
 - Step 3** Click **Run License Audit**.
 - Step 4** In the **Run License Audit** dialog box, click **Submit**.
This process takes some time to complete.
 - Step 5** In the confirmation dialog box, click **OK**.
-

Authentication and LDAP Integration

You can configure an authentication preference with a fallback choice for LDAP. You can also configure a preference with no fallback for Verisign Identity Protection (VIP) authentication.

Name	Description
Local First, fallback to LDAP	Authentication is done first at the local server (Cisco IMC Supervisor). If the user is unavailable at the local server, the LDAP server is checked.
Verisign Identity Protection	VIP Authentication Service (two-factor authentication) is enabled.

Configuring Authentication Preferences

Perform this procedure when you want to change the login authentication type.

Procedure

-
- Step 1** From the menu bar, choose **Administration > Users and Groups**.
 - Step 2** Choose the **Authentication Preferences** tab
 - Step 3** From the **Authentication Preferences** drop-down list, you can choose one of the following options:
 - **Local First, fallback to LDAP**

If you select this option, then you must configure LDAP servers. For more information, see [Configuring LDAP Servers, on page 8](#).

- **Verisign Identity Protection**— If you select this option, continue to the next step.

Step 4 If you select Verisign Identity Protection, complete the following steps:

- a) Click **Browse** to upload a VIP certificate.
Locate and select the certificate, and click **Upload**.
- b) Enter the **Password**.

Step 5 Click **Save**.

Configuring LDAP

Configuring LDAP in Cisco IMC Supervisor involves adding LDAP configurations and configuring LDAP servers. You can also test the LDAP connectivity and view LDAP summary information. The following sections explain how to perform these procedures.

LDAP Integration Rules and Limitations

Group Synchronization Rules

- If a chosen LDAP group already exists in Cisco IMC Supervisor and the source is type **Local**, the group is ignored during synchronization.
- If a chosen LDAP group already exists in Cisco IMC Supervisor and the group source is type **External**, the group's description and email attributes are updated in Cisco IMC Supervisor.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a group filter, all users that belong to the specified group are added to the system. In addition, the following actions are also performed:
 - If the specified group includes sub-groups, then the group, the sub-groups and the users in those sub-groups are added to the system (only applicable when you manually synchronize the LDAP directory).
 - If the user is part of multiple groups, and the other groups do not match the group specified as the group filter, then those additional groups are not added to the system.
- A user can be part of multiple user groups. However, the group that is mentioned first in the list of groups that the user is part of is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**.



Note You can view information on all the groups that a user is part of only after the **LDAPSyncTask** system task is run.

- When an LDAP group is synchronized, all users that are in the group are first added to the system. Also, if users in the specified LDAP group are associated with other groups that are in the same OU or in a different OU, then those groups are also retrieved and added to the system.
- The LDAP synchronization process will retrieve the specified LDAP groups for the system, along with nested groups, if any.
- Prior to this release, a user was part of only one group. After an upgrade to the current release, and only after the **LDAPSycTask** system task is run, the **Manage Profiles** dialog box displays the other groups that the user is part of. This is applicable only when the other groups match the group filters that you specified while configuring the LDAP server.

User Synchronization Rules

- LDAP users that have special characters in their names are now added to Cisco IMC Supervisor.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a user filter, all the users that match the filter you specified, and the groups that they belong to, are retrieved for the system.
- Cisco IMC Supervisor now displays the User Principal Name (UPN) for each user that is added into the system. This is applicable for users that have been added into the system in prior releases. Users can log in to the system using their login name or their user principal name. Logging in using the user principal name along with the profile name is not supported.
- If a chosen LDAP user already exists in Cisco IMC Supervisor and the source is type **Local**, the user is ignored during synchronization.
- If a chosen LDAP user already exists in Cisco IMC Supervisor and the source type is **External**, the user's name, description, email, and other attributes are updated for use.
- If a user account is created in two different LDAP directories, then the user details of the LDAP directory that was synchronized first is displayed. The user details from the other LDAP directory is not displayed.
- After LDAP directories are synchronized, the LDAP external users must login to Cisco IMC Supervisor by specifying the complete domain name along with the user name. For example, `vxdomain.cisco.com\username`. However, this rule does not apply if there is only one LDAP server directory added to Cisco IMC Supervisor.

User Synchronization Limitations

- If a user has multiple group membership, that user has single group membership in Cisco IMC Supervisor.



Note

- We recommend to keep the total number of users and groups (both local and LDAP) in Cisco IMC Supervisor to 10,000 or less. If this number is exceeded, the appliance may become slow or unresponsive.
- After an LDAP synchronization process, verify that the user is assigned to the correct group.

Best Practices

The synchronization of thousands of LDAP objects to Cisco IMC Supervisor can lead to some performance issues in the appliance. Use the following procedure to synchronize only the required LDAP objects.

- 1 Create LDAP groups that contain all users that should have access to Cisco IMC Supervisor.
- 2 Synchronize only those groups to Cisco IMC Supervisor.

Adding LDAP Configurations

Perform this procedure to add LDAP configurations.

Procedure

- Step 1** From the menu bar, choose **Administration > LDAP Integration**.
- Step 2** Click + to add LDAP configurations.
- Step 3** In the **Add LDAP Configurations** dialog box, complete the following fields:

Field	Description
Account Name field	An LDAP account name.
Server Type drop-down list	Choose either Microsoft Active Directory or Open LDAP.
Server field	Host name or the IP address of the server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name for the LDAP user.
Username field	Enter a name for the LDAP user.
Password field	Enter a password associated with the username.
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAPserver must be synchronized. It can be one of the following: <ul style="list-style-type: none"> • 1 • 4 • 12 • 24

- Step 4** Click Next.
- Step 5** In the **LDAP Search Base** dialog box, click **Select** and choose search criteria for retrieving users based on OU from the table displayed.

Note Cisco IMC Supervisor supports only users and not groups. Search criteria is not mandatory based on **OU** as it can have both users as well as groups. The system sync up task runs every 24 hours and syncs up LDAP users based on the search criteria. Hence, you must perform a manual sync of only user information. To perform a manual LDAP sync, refer [Requesting Manual LDAP Sync, on page 12](#).

- Step 6** Click **Select** in the **Select** dialog box.
The search criteria you have selected is displayed next to the **Search Base** field.
- Step 7** Click **Next** in the **LDAP Search Base** dialog box.
- Step 8** Click + to add entry to user role filters table in the **LDAP User Role Filter** dialog box.
- Step 9** Enter the user role details in the **Add Entry to User Role Filters** dialog box.
- Step 10** Click **Submit**.
- Step 11** In the **Submit Result** dialog box, click **OK**.
You can edit or delete these filters. You can also use the up or down arrows to move the filters to set priority.
- Step 12** Click **Submit** in the **LDAP User Role Filter** dialog box.
- Step 13** In the **Submit Result** dialog box, click **OK**.
-

Configuring LDAP Servers

You can configure multiple LDAP servers and accounts in Cisco IMC Supervisor. While adding LDAP accounts, you can specify the following:

- An organization unit (OU) that is part of the search base distinguished name (DN).
- A frequency at which the LDAP account is automatically synchronized with the system.
- A group or user filter to limit the results, and specify an LDAP role filter on the groups and users

Soon after an LDAP server account is added, a system task for this account is created automatically, and it immediately begins to synchronize the data. All the users and groups in the LDAP server account are added to the system. By default, all the users from the LDAP account are automatically assigned to the service end-user profile.

Before You Begin

You should have set the authentication preferences to **Local First, fallback to LDAP**.

Procedure

- Step 1** From the menu bar, choose **Administration > LDAP Integration**.
- Step 2** Click **Add**.
- Step 3** In the **LDAP Server Configuration** dialog box, complete the following fields:

Name	Description
Account Name field	The name of the account. This name must be unique.

Name	Description
Server Type field	<p>The type of LDAP server. It can be one of the following:</p> <ul style="list-style-type: none"> • OpenLDAP • MSAD - Microsoft Active Directory
Server field	The IP address or the host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	<p>The port number.</p> <p>It is automatically set to 636 for SSL, and 389 for non-secure mode.</p>
Domain Name field	<p>The domain name.</p> <p>If you selected OpenLDAP as the LDAP Directory Type, then this domain name must match the domain specified with the user name.</p> <p>Important You must specify the complete domain name. For example, vxedomain.com.</p>
User Name field	<p>The user name.</p> <p>If you selected OpenLDAP as the LDAP Directory Type, then specify the user names in the following format:</p> <p>uid=users,ou=People,dc=ucsd,dc=com</p> <p>where ou specified is the one all the other users are placed in the directory hierarchy.</p>
Password field	The user password.
Synchronization Frequency drop-down list	<p>Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following:</p> <ul style="list-style-type: none"> • 1 • 4 • 12 • 24

Step 4 Click Next.

Step 5 In the **LDAP Search Base** pane, click **Select** to specify LDAP search base entries and click **Select**.

All organization units (OU) that are available in Cisco IMC Supervisor are displayed in this list.

Step 6 Click **Next**.

Step 7 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the groups you have selected are retrieved and added into the system. However, if the users in the group you have selected are also part of other non-selected groups, then those groups are not retrieved unless they are also selected in this field.
Add Entry to User Filters or Add Entry to Group Filters dialog box (displayed based on your previous selection)	
Attribute Name drop-down list	Choose either Group Name or User Name .
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: <ul style="list-style-type: none"> • Equals to • Starts with
Attribute Value field	Specify a keyword or a value that must be included in the search.

Based on the filters, the groups or users are retrieved.

Step 8 Click **Next**.

Step 9 In the **LDAP User Role Filter** pane, click the + sign to add a user role filter.

Step 10 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be Group Name .
Operator drop-down list	The drop-down list can be one of the following: <ul style="list-style-type: none"> • Equal to • Starts with

Name	Description
Attribute Value field	Specify a value in this field. All users that match the values of the Operator field and the Attribute Value field are assigned to the user role you select in the Map User Role drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco IMC Supervisor: <ul style="list-style-type: none"> • Group Admin • Operator • System Admin

Step 11 Click **Submit**.

Step 12 Click **OK**.

The user role filters are added to the **User Role Filters** table.

Note If you have multiple user role filters specified, then the filter specified in the first row is processed.
If you manually update the role for a user, then the user role that you earlier mapped the group to, is no longer applied on the user.

What to Do Next

If you have not set the authentication preference to LDAP, then you are prompted to modify the authentication preference. For more information on changing the authentication preference, see [Configuring Authentication Preferences](#), on page 4.

Viewing LDAP Server Summary Information

Perform this procedure to view the summary information of the LDAP server.

Procedure

Step 1 From the menu bar, choose **Administration > LDAP Integration**.

Step 2 Choose an LDAP account name from the table.

Step 3 Click **View**.

The **View LDAP Account Information** dialog box displays summary information of the LDAP account.

Step 4 Click **Close**.

Testing LDAP Server Connectivity

Perform this procedure to test the LDAP connection.

Procedure

- Step 1** From the menu bar, choose **Administration > LDAP Integration**.
 - Step 2** Choose an LDAP account name from the table.
 - Step 3** Click **Test Connection**.
The status of the connection is displayed.
 - Step 4** Click **Close** in the **Test LDAP Connectivity** dialog box.
-

Searching BaseDN

Perform this procedure to search the BaseDN.

Procedure

- Step 1** From the menu bar, choose **Administration > LDAP Integration**.
 - Step 2** Click **Search BaseDN**.
Note Cisco IMC Supervisor supports only users and not groups. Search criteria is not mandatory based on **OU** as it can have both users as well as groups.
 - Step 3** Click **Select** in the **LDAP Search Base** dialog box.
 - Step 4** Choose one or more users and click **Select** in the **Select** dialog box.
 - Step 5** Click **Submit** in the **LDAP Search Base** dialog box.
 - Step 6** In the **Submit Result** dialog box, click **OK**.
-

Requesting Manual LDAP Sync

Requesting manual LDAP synchronization enables you to specify either basic or advanced search criteria to retrieve LDAP users and groups. Perform this procedure for manual LDAP synchronization.

Procedure

Step 1 From the menu bar, choose **Administration > LDAP Integration**.

Step 2 Click **Request Manual LDAP Sync**.

Step 3 In the **Manual LDAP Sync** dialog box, complete the following fields:

Name	Description
Basic Search check box	Enables basic search by organization unit.
Advanced Search check box	Enables advanced search.

Note When you use either of the search options, if the users and groups already exist in Cisco IMC Supervisor, then the same users and groups are not populated after performing the search.

Step 4 For basic search, click **Select** to specify the search base.

Step 5 Choose the search base DN, and click **Select** and continue to Step 9.

Step 6 For advanced search, in the **Advanced Filtering Options** pane, add or edit attribute names for **User Filters** and **Group Filters**.

Step 7 Click **Next**.

Step 8 In the **Select Users and Groups** dialog box, complete the following fields:

Name	Description
LDAP Groups field	The LDAP groups from which the users must be synchronized.
LDAP Users field	The LDAP users that must be synchronized.

Step 9 Click **Submit**.

Step 10 In the **Submit Result** dialog box, click **OK** to synchronize the LDAP server.
From the menu bar, choose **Administration > Users and Groups** and click **Users** tab to see the synchronized users.

Viewing LDAP Synchronized Results

Perform this procedure to view the LDAP synchronized results.

Procedure

-
- Step 1** From the menu bar, choose **Administration > Users and Groups**.
 - Step 2** Click the **LDAP Integration** tab and select an LDAP account.
 - Step 3** Click **Results**.
 - Step 4** Click the **License Status** tab to view the validity of the Cisco IMC Supervisor license.
 - Step 5** Click the **LDAP Integration** tab to view the details such as the start and end time of LDAP synchronization, status of synchronization and a detailed message of the status.
-

Modifying LDAP Server Details

You can only modify the following details for a configured LDAP server:

- Port numbers and SSL configuration
- User name and password
- Search BaseDN selections

Perform the following procedure to modify the LDAP server details.

Procedure

-
- Step 1** From the menu bar, choose **Administration > Users and Groups**.
 - Step 2** Click the **LDAP Integration** tab and select an LDAP account.
 - Step 3** Click **Modify**.
 - Step 4** In the **Modify LDAP Server Configuration** dialog box, edit the following fields:

Name	Description
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
User Name field	The user name. If you selected OpenLDAP as the LDAP Directory Type, then specify the user names in the following format: uid=users,ou=People,dc=ucsd,dc=com where ou specified is the one all the other users are placed in the directory hierarchy.

Name	Description
Password field	The user password.

- Step 5** Click **Next**.
- Step 6** In the **LDAP Search Base** dialog box, click **Select** to specify LDAP search base entries and click **Select**.
- Step 7** Click **Next**.
- Step 8** In the **Configure User and Group Filters** pane, select and edit the required attributes in the **User Filters** and **Group Filters** table.
- Step 9** Click **Next**.
- Step 10** In the **LDAP User Role Filter** dialog box, click add, edit, delete, or move table entries using up and down arrows.
- Step 11** Click **Submit** in the respective dialog boxes.
- Step 12** In the **Submit Result** dialog box, click **OK**.
- Step 13** Click **Submit** in the **LDAP User Role Filter** dialog box.
- Step 14** In the **Submit Result** dialog box, click **OK**.

Deleting LDAP Server Information

Deleting an LDAP server account only results in deleting the search criteria, BaseDNs, and system entries related to this LDAP server. Users attached to the LDAP server are not deleted. Perform this procedure to delete the LDAP server information.

Procedure

- Step 1** From the menu bar, choose **Administration > Users and Groups**.
- Step 2** Choose the **LDAP Integration** tab.
- Step 3** Choose an LDAP account name from the table.
- Step 4** Click **Delete**.
- Step 5** In the confirmation dialog box, click **Delete**.
- Step 6** Click **OK**.
- This initiates the deletion of the LDAP account in Cisco IMC Supervisor. Based on the number of users in the LDAP account, this deletion process could take a few minutes to complete. During such time, the LDAP account may still be visible in Cisco IMC Supervisor. Click **Refresh** to ensure that the account has been deleted.

Configuring a SCP User

SCP user is used by server diagnostics and tech support upload operations for transferring file to the Cisco IMC Supervisor appliance using SCP protocol. An scp user account cannot be used to login to the Cisco IMC Supervisor UI or the shelladmin. Perform this procedure for configuring scp user password.

Procedure

-
- Step 1** From the menu bar, choose **Administration > Users and Groups**.
 - Step 2** Click the **SCP User Configuration** tab.
 - Step 3** Enter the scp user password in the **Password** field.
 - Step 4** Click **Submit**.
 - Step 5** In the **Submit Result** dialog box, click **OK**.
-

Configuring Mail Setup

All outgoing emails from Cisco IMC Supervisor require an SMTP server. Cisco IMC Supervisor generated emails such as alerts for faults and so on are sent to the mail setup you have configured using the following procedure. For more information about adding email alert rules, see [Adding Email Alert Rules for Server Faults](#).

Procedure

-
- Step 1** From the menu bar, choose **Administration > System**.
 - Step 2** Click the **Mail Setup** tab.
 - Step 3** In the **Mail Setup** pane, complete the following fields:

Field	Description
Outgoing Email Server (SMTP)	IP address of the server or the domain name.
Outgoing SMTP Port	Port number for the SMTP server.
Outgoing SMTP User	(Optional) The outgoing SMTP user ID to use for SMTP authentication.
Outgoing SMTP Password	(Optional) The password for the outgoing SMTP user ID to use for SMTP authentication.
Outgoing Email Sender Email Address	The From address of the outgoing Cisco IMC Supervisor generated emails.
Server IP Address	IP address of the server running Cisco IMC Supervisor.

Field	Description
Send Test Email checkbox	Check this check box to send a test email to the configured address.

Step 4 Click **Save**.

Step 5 In the confirmation dialog box, click **OK**.

Branding

A login page can be configured to display a logo that is associated with a domain name. When the end user logs in from that domain, the user sees the custom logo on the login page. The optimal image size for a logo is 890 pixels wide and 470 pixels high, with 255 pixels allowed for white space. Cisco recommends that you keep the image size small to enable faster downloads.

Adding New Login Branding Page

Perform this procedure when you want to add a new login branding page.

Procedure

Step 1 From the menu bar, choose **Administration > Users and Groups**.

Step 2 Click the **Login Page Branding** tab.

Step 3 Click **Add**.

Step 4 In the **Domain Branding** dialog box, complete the following:

Field	Description
Domain Name field	A domain name for branding. For example, imcs.xxxx.com. Note For creating a domain name in your local machine, navigate to C:\Windows\System32\drivers\etc and specify the <ipaddress> and <domainname> in the hosts file. For example, 10.10.10.10 imcs.xxxx.com.
Custom Domain Logo checkbox	(Optional) If you want to add a logo, check this checkbox and do the following: <ol style="list-style-type: none"> 1 Click Browse. 2 Navigate to a logo and choose the file. 3 Click Open.

Step 5 Click **Submit**.

Step 6 In the confirmation dialog box, click **OK**.

Note You can edit, delete, and clone the customized login page you have created.

Configuring User Interface Settings

You can use this procedure to customize the Cisco IMC Supervisor application. You can modify the application header, the administrator and end-user portal based on your requirement. The header containing the logo, application name, and links such as logout can also be hidden.

Procedure

Step 1 From the menu bar, choose **Administration > User Interface Settings**.

Step 2 In the **User Interface Settings** window, complete the following:

Field	Description
Hide Entire Header check box	Use this check box to enable or disable the header.
Product Name field	Main title of the header.
Product Name 2nd Line field	Sub-title of the header.
Enable About Dialog checkbox	Use this checkbox to enable or disable the About dialog box for Cisco IMC Supervisor.
Administrator Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the Custom Link 1 Lable
Custom Link 2 Lable field	You can configure this field to change the text on header bar.
Custom Link 2 URL field	You can configure the URL for the Custom Link 2 Lable
End-user Portal	
Custom Link 1 Lable field	You can configure this field to change the text on header bar.
Custom Link 1 URL field	You can configure the URL for the Custom Link 1 Lable
Custom Link 2 Lable field	You can configure this field to change the text on header bar.
Custom Link 2 URL field	You can configure the URL for the Custom Link 2 Lable

- Step 3** Click **Save**.
- Step 4** In the confirmation dialog box, click **OK**.
-

