



Access Control Configuration

- [Access Control](#), on page 1
- [Administrator and User Accounts](#), on page 1
- [User Access Attribute](#), on page 2
- [User Preference Attribute](#), on page 2
- [Access the Phone Web Interface](#), on page 3
- [Enable HTTPS by Default](#), on page 3
- [Control Access to the Phone Settings](#), on page 4
- [Bypass the Set Password Screen](#), on page 8

Access Control

If the <Phone-UI-User-Mode> parameter is enabled, the phone GUI honors the user access attribute of the relevant parameters when the GUI presents a menu item.

For menu entries that are associated with a single configuration parameter:

- Provisioning the parameter with “ua=na” (“ua” stands for “user access”) attribute makes the entry disappear.
- Provisioning the parameter with “ua=ro” attribute makes the entry read-only and non-editable.

For menu entries that are associated with multiple configuration parameters:

- Provisioning all concerned parameters with “ua=na” attribute makes the entries disappear.

Administrator and User Accounts

The Cisco IP Phone firmware provides specific administrator and user accounts. These accounts provide specific login privileges. The administrator account name is **admin**; the user account name is **user**. These account names cannot be changed.

The **admin** account gives the service provider or Value-added Reseller (VAR) configuration access to the Cisco IP phone. The **user** account gives limited and configurable control to the device end user.

The **user** and **admin** accounts can be password protected independently. If the service provider sets an administrator account password, you are prompted for it when you click **Admin Login**. If the password does

not yet exist, the screen refreshes and displays the administration parameters. No default passwords are assigned to either the administrator or the user account. Only the administrator account can assign or change passwords.

The administrator account can view and modify all web profile parameters, including web parameters, that are available to the user login. The Cisco IP Phone system administrator can further restrict the parameters that a user account can view and modify through use of a provisioning profile.

Configuration parameters that are available to the user account are configurable on the Cisco IP Phone. User access to the phone web user interface can be disabled.

User Access Attribute

The user access (**ua**) attribute controls may be used to change access by the User account. If the **ua** attribute is not specified, the existing user access setting is retained. This attribute does not affect access by the Admin account.

The **ua** attribute, if present, must have one of the following values:

- na—No access
- ro—Read-only
- rw—Read and write
- y—Preserve value

The **y** value must be used together with **na**, **ro**, or **rw**.

The following example illustrates the **ua** attribute. Notice in the last line that the **ua** attribute is updated to **rw**, and the station name field (**Travel Agent 1**) is preserved. If **y** is not included, **Travel Agent 1** is overwritten:

```
<flat-profile>
  <SIP_TOS_DiffServ_Value_1_ ua="na"/>
  <Dial_Plan_1_ ua="ro"/>
  <Dial_Plan_2_ ua="rw"/>
<Station_Name ua="rw" preserve-value="y">Travel Agent 1</Station_Name></flat-profile>
```

Double quotes must enclose the value of the **ua** option.

User Preference Attribute

user-pref attribute allows you to set some user preferred value to provide a seamless experience for your user. However, user can make further changes from the phone or from the phone administration web page. Any parameter changed by user is marked as user modified with an attribute **um**. Any changes made by the user is preserved. **user-pref** can be updated during provisioning using XML configurations delivered with **Profile Rule** parameter.

The **user-pref** attribute is not mandatory. However, if present, must have one of the following values:

- y—indicates to honor the user made changes to be included during the configuration. It also specifies to set the value set by the administrator if the user has not modified it.
- n—indicates to honor administrator set value provided through XML configurations. If **user-pref** attribute is not included, the **user-pref** attribute has the same effect as setting its value to "n".

The following example illustrates the **user-pref** attribute.

```
<flat-profile>
  <Display_Brightness ua="rw" user-pref="y">5</Display_Brightness>
</flat-profile>
```

If the user modifies the value, the change is tracked as **um**="y". **um** attribute can't be updated by provisioning using **um** and it is visible in the XML configurations pulled from the phone.

The following example illustrates the **um** attribute.

```
<flat-profile>
  <Display_Brightness ua="rw" user-pref="y" um="y">5</Display_Brightness>
</flat-profile>
```

Factory reset clears all the configurations marked with **um** and **user-pref** attributes.

During provisioning, for any parameter, if attribute **user-pref**="n" is added, after you apply the configuration, the parameter's attribute **user-pref** is updated to "n", also **um** gets cleared.

Access the Phone Web Interface

The phone firmware provides mechanisms for restricting end-user access to some parameters. The firmware provides specific privileges for sign-in to an **Admin** account or a **User** account. Each can be independently password-protected.

- Admin account—Allows the full access to all administration web server parameters
- User account—Allows the access to a subset of the administration web server parameters

If your service provider has disabled access to the configuration utility, contact the service provider before proceeding.

Procedure

- Step 1** Ensure that the computer can communicate with the phone. No VPN in use.
- Step 2** Start a web browser.
- Step 3** Enter the IP address of the phone in your web browser address bar.
- User Access: **http://<ip address>**
 - Admin Access: **http://<ip address>/admin/advanced**
 - Admin Access: **http://<ip address>**, click **Admin Login** and click **advanced**

For example, <https://10.64.84.147/admin>

- Step 4** Enter the password when prompted.
-

Enable HTTPS by Default

You must enable **Https** by default to access the phone administration web page.

- You set the value of **Enable Protocol** to **Https** and **Web Server Port** to **443** and factory reset the phone. After factory reset both the values remain unchanged and if your user wants to access the phone

administration web page with `http://<ip address>` or `http://<ip address>:80`, the URL gets redirected to `https://<ip address>:443`. when HTTPS is set as default.

- If the phone upgrades to Firmware release 12.0(3), and you change values of the parameters, the url will still redirect to `https://phone IP:443` by default to access the phone administration web page.
- After factory reset, if you change **Web Server Port** to **80** and **Enable Protocol** to **Https**, the user can't access the phone administration web page with `http://phone IP:80` but can access the page with `https://phone IP:80`.
- If the phone upgrades to Firmware release 12.0(3), the user can only access the phone administration web page using **https** protocol.

Before you begin

- Access the phone administration web page. See [Access the Phone Web Interface, on page 3](#).

Procedure

Step 1 Select **Voice > System**.

Step 2 In the **System Configuration** section, set **Enable Protocol** parameter to **Https** and **Web Server Port** parameter to **443**.

You can also enable the parameters in the phone configuration file (cfg.xml).

```
<Enable_Protocol ua="na">Https</Enable_Protocol>
<Web_Server_Port ua="na">443</Web_Server_Port>
```

Step 3 Click **Submit All Changes**.

Control Access to the Phone Settings

You can configure the phone to allow or block access to the configuration parameters on the phone web page or the phone screen. The parameters for access control allow you to:

- Indicate which configuration parameters are available to the user account when creating the configuration.
- Enable or disable the access to the administration web server.
- Enable or disable user access to the phone screen menus.
- Bypass the **Set password** screen for the user.
- Restrict the Internet domains that the phone accesses for resync, upgrades, or SIP registration for Line 1.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in [Access Control Parameters, on page 5](#).

Before you begin

Access the phone administration web page. See [Access the Phone Web Interface, on page 3](#).

Procedure


-
- Step 1** Click **Voice > System**.
- Step 2** In the **System Configuration** section, configure the parameters as defined in the [Access Control Parameters, on page 5](#) table.
- Step 3** Click **Submit All Changes** to apply the changes.
-

Access Control Parameters

The following table defines the function and usage of the access control parameters in the **System Configuration** section under the **Voice > System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 1: Access Control Parameters

Parameter Name	Description and Default Value
Enable Web Server	<p>Enables or disables access to the phone web interface. Set this parameter to Yes to allow users or administrators to access the phone web interface. Otherwise, set it to No. When set to No, the phone web interface isn't accessible.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre><Enable_Web_Server ua="na">Yes</Enable_Web_Server></pre> In the phone web interface, set to Yes to allow the access. <p>Allowed values: Yes No</p> <p>Default: Yes.</p>

Parameter Name	Description and Default Value
Enable Web Admin Access	<p>Allows or blocks the access to the phone administration pages:</p> <p>http://<phone_IP>/admin</p> <p>When set to No, the web page for administrator is inaccessible. Only the web page for user is accessible.</p> <p>Note If you want to allow the access to the administration web page again after the access is blocked, you need to perform a factory reset from the phone.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre><Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access></pre> In the phone web interface, set this parameter to Yes to allow the access. Otherwise, set it to No. <p>Allowed values: Yes No</p> <p>Default: Yes</p>
Admin Password	<p>Allows you to set or change the password for accessing the phone administration web pages.</p> <p>The Admin Password parameter is only available on the phone administration web page.</p> <p>A valid password must contain 4 to 127 characters from three out of the four types: capital letter, small letter, number, and special character.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre><Admin_Password ua="na">P0ssw0rd_tes89</Admin_Password></pre> In the phone web interface, enter the password for administrator access. <p>Default: Empty</p>
User Password	<p>Allows you or the phone user to set or change the password for accessing the phone web interfaces and the menus on the phone screen.</p> <p>You can also set or change the user password from the phone screen menu Applications  > Device administration > Set password.</p> <p>A valid password must contain 4 to 127 characters from three out of the four types: capital letter, small letter, number, and special character.</p> <p>In the configuration file (cfg.xml), you can use the User_Password parameter to bypass the Set password screen that prompts on the first boot or after a factory reset. For more information, see Bypass the Set Password Screen, on page 8.</p> <p>Default: Empty</p>

Parameter Name	Description and Default Value
Phone-UI-User-Mode	<p>This parameter works only with the user access the (ua) attribute attached to an element tag in the configuration file (cfg.xml). You can restrict the parameters that the phone users see on the phone screen.</p> <p>When set to Yes, you can use the ua attribute to control user access to specific parameters on the phone screen menu. When set to No, the ua attribute isn't working.</p> <p>The options for the ua attribute are "na", "ro", and "rw". Parameters designated as "na" don't appear on the phone screen. Parameters designated as "ro" aren't editable by the user. Parameters designated as "rw" are editable by the user.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> • In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="672 695 1321 720"><Phone-UI-User-Mode ua="na">No</Phone-UI-User-Mode></pre> • In the phone web interface, set to Yes and then set the ua attribute of the desired parameter in the phone configuration file. <p>Example:</p> <pre data-bbox="618 873 1435 972"><Phone-UI-User-Mode ua="na">Yes</Phone-UI-User-Mode> <Enable_VLAN ua="ro">Yes</Enable_VLAN> <Preferred_Audio_Device ua="rw">Headset</Preferred_Audio_Device> <Block_ANC_Setting ua="na">Yes</Block_ANC_Setting></pre> <p>With the settings in the example, the user:</p> <ul style="list-style-type: none"> • Can see but can't change the setting of VLAN (<code>Enable_VLAN</code>) on the phone screen menu • Can change the setting of Preferred audio device (<code>Preferred_Audio_Device</code>) • Can't see the menu item Block anonymous call (<code>Block_ANC_Setting</code>) on the phone screen. <p>Allowed values: Yes No Default: No</p>
User Password Prompt	<p>Controls whether the user password setup screen prompts.</p> <p>Perform one of the following:</p> <ul style="list-style-type: none"> • In the phone configuration file with XML(cfg.xml), enter a string in this format: <pre data-bbox="672 1522 1386 1547"><User_Password_Prompt ua="na">Yes</User_Password_Prompt></pre> • In the phone web interface, set to Yes to make the prompt available to the user. <p>Allowed values: Yes No Default: Yes</p>

Bypass the Set Password Screen



Note This feature isn't available from firmware release 11.2.3 and later.

You can bypass the phone **Set password** screen on the first boot or after a factory reset, based on these provisioning actions:

- DHCP configuration
- EDOS configuration
- User password configuration using in the phone XML configuration file

After the User Password is configured, the set password screen doesn't appear.

Procedure

Step 1 Edit the phone `cfg.xml` file in a text or XML editor.

Step 2 Insert the `<User_Password>` tag using one of these options.

- No password (start and end tag) `<User_Password></User_Password>`
- Password value (4-127 characters) `<User_Password >Abc123</User_Password>`
- No password (start tag only) `<User_Password />`

Step 3 Save the changes to the `cfg.xml` file.

The **Set password** screen doesn't appear on the first boot or after a factory reset. If a password is specified, the user is prompted to enter the password when accessing the phone web interface or the phone screen menus.