Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuration and Maintenance of Cisco Unified Presence

- Changing Cisco Unified Communications Manager Publisher Information

- Configuring Application Listeners on Cisco Unified Presence

- How to Configure Access Control Lists (ACL) on Cisco Unified Presence

Changing Cisco Unified Communications Manager Publisher Information

Cisco Unified Presence is dependent upon Cisco Unified Communications Manager for configuration of users, devices, and licensing. The Cisco Unified Presence publisher communicates with the Cisco Unified Communications Manager publisher via the AVVID XML Layer Application Programming Interface (AXL API).

You can change the Cisco Unified Communications Manager publisher address and IP security password that you first configured. You can also reconfigure the username and password for AXL API access to the associated Cisco Unified Communications Manager publisher node.

However, for the Sync Agent to work properly, the AXL username and password must match the AXL username and password that is configured on the associated Cisco Unified Communications Manager publisher node.

Before You Begin

- Obtain the Cisco Unified Communications Manager hostname or IP address
- Obtain the Cisco Unified Communications Manager AXL username and password
- Configure the Cisco Unified Communications Manager publisher node. The status poller on the Cisco Unified Communications Manager Publisher window checks Cisco Unified Communications Manager (via AJAX-AXL) every 60 seconds for status.

Procedure

1. Select System **> CUCM Publisher**.
2. Enter the following data:
   - a valid Cisco Unified Communications Manager publisher hostname
   - a valid IP address
   - a security password for the Cisco Unified Communications Manager publisher. Confirm this password.
   - the AXL username and password. Confirm this password.
3. Review the publisher status, and repeat Step 2 if the publisher node configuration failed.

Table 1: Publisher Node Status

Field	Description
Publisher Reachability (pingable)	If successful, the Cisco Unified Communications Manager publisher can be reached (pingable). If a failure occurs, the Cisco Unified Communications Manager publisher can not be reached over the network.
Peer Connectivity (via AXL)	If successful, the AXL connection to the Cisco Unified Communications Manager publisher was successful. If a failure occurs, the system is unable to connect to the CUCM publisher via AXL.
Publisher Security Login (IPSec)	If successful, the security password used to connect to the Cisco Unified Communications Manager publisher was successful. If a failure occurs, the system is unable to connect using the security password you entered.
Publisher Version	If successful, the version of the Cisco Unified Communications Manager publisher is displayed.

4. Select **Save**.

Troubleshooting Tips

- You must enter the User ID and password for the application user that has the Standard AXL API Access role assigned to it on the associated Cisco Unified Communications Manager first node. By default, the Standard AXL API Access role is assigned to the CCMAdministrator User ID.

- If an error message displays, you can check that AXL is running on Cisco Unified Communications Manager and that you have the correct User ID and password. Using a browser, enter http://<<CUCM Hostname>>/axl. You will be prompted for the User ID and password. If the details that you enter are correct, a web page displays confirmation that AXL is running and ready to receive requests.
- When you save your data, a popup displays to alert you to restart your system to synchronize the data.

Related Topics

- Completing Cisco Unified Presence Post-Installation Setup
- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

Configuring Application Listeners on Cisco Unified Presence

You can configure application listeners for the SIP proxy server, presence engine, and profile agent. The system binds each application listener to a specific address and port combination. If you choose TLS protocol, you must also choose a TLS context.

Procedure

1. Perform one of the following actions:

If you want to:	Action
Add an application listener	1. Select **System > Application Listeners**. 2. Select **Add New**.
Update an application listener	1. Find the record. See the Finding a Network Component topic for instructions. 2. Edit the record as required.

2. Enter the application listener configuration settings as described in the table below.

Field	Description
Listener Type	Specifies the type of application listener: ◊ SIP ◊ HTTP ◊ HTTPS
Name	Specifies the unique name of this listener. Maximum characters: 128
Port	Specifies the port number that is configured for this listener.

	Default Port: 5060
Service Type	Specifies the service type of this application listener: ◊ Cisco Proxy Server ◊ Cisco Presence Engine ◊ Cisco Unified Client Profile Agent Default Setting: Cisco Proxy Server
Transport Type	Specifies the type of protocol that this listener will use, TCP, UDP, or TLS. Default Setting: UDP
TLS Context	Specifies the TLS context that is associated with this listener and only applies when you select the TLS protocol type. **Note:** The available TLS contexts are configured in the TLS Context Configuration window.

3. Select **Save**.

Troubleshooting Tips

- You must restart the SIP proxy server before any changes that you make to the application listeners take effect. To restart the proxy server, select Presence **> Routing > Settings**.
- For Cisco Proxy Server listeners, there is a limit of 20 listeners.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

How to Configure Access Control Lists (ACL) on Cisco Unified Presence

- Allowed ACL Formats
- Configuring Incoming and Outgoing ACL

Allowed ACL Formats

In the Incoming and Outgoing Access Control List (ACL), you can configure patterns that control which incoming hosts and domains can access Cisco Unified Presence without authentication. Cisco Unified Presence accepts a range of IP address patterns in addition to fully qualified names of incoming hosts or domains. The Allow directive followed by "from" determines which hosts can access the server.

When configuring incoming and outgoing ACL settings, you can select from the formats described in Table 2: ACL Address Patterns.

Table 2: ACL Address Patterns

Host Address Description	Configuration Example
All hosts	• Allow from all
A partial domain name	• Allow from company.com
A full IP address	• Allow from 10.1.2.3
A partial IP address	• Allow from 10.1
A network/netmask pair	• Allow from 10.1.0.0/255.255.0.0
A network/nnn CIDR specification	• Allow from 10.1.0.0/16 **Note:** The netmask consists of nnn high-order 1 bits.

Configuring Incoming and Outgoing ACL

Before You Begin

- Configure an address which will be added to the SIP Proxy list of allowed incoming and outgoing addresses. Any address added to this list will bypass digest authentication.
- Once you add a federated domain entry to the database, Cisco Unified Presence automatically adds an incoming ACL entry for the federated domain. You do not need to manually perform these configuration steps.
- By default, system behavior is to deny all incoming and outgoing requests. If you check the CUP CVP Support checkbox in the Presence > Settings window, you are allowed to modify the default system-generated entries.

Procedure

1. Perform one of the following actions:

Table 3: Incoming ACL Configuration Settings

If you want to:	Action
Add an incoming or outgoing ACL	1. Perform one of the following actions: ◊ Select **System > Security > Incoming ACL**. ◊ Select **System > Security > Outgoing ACL**. 2. Select **Add New**.
Update an incoming ACL entry	1. Find the record. See the Finding a Network Component topic for instructions. 2. Edit the record as required.

2. Enter the incoming or outgoing ACL configuration settings as described in Table 3: Incoming ACL Configuration Settings.

Field	Description
Description	Specifies a general description of the ACL entry. Maximum characters: 128
Address Pattern	Specifies the address or pattern of the incoming and outgoing host or domain as either an IP address or a Fully Qualified Domain Name (FQDN).

3. Select **Save**.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information