External Authentication Integration

External authentication integration in Crosswork enables secure user access management by connecting the platform to enterprise authentication systems such as TACACS+, LDAP, and RADIUS.

This chapter provides an overview of supported external authentication options, essential configuration principles, and the procedures required to control and monitor user sign-on through centralized authentication and authorization services.

User authentication systems

A user authentication system is a security feature that

- verifies user identities through external servers such as TACACS+, LDAP, or RADIUS,
- centralizes account and role management across the organization, and
- enables administrators to enforce consistent access policies for all users.

External authentication allows Crosswork Network Controller to delegate credential verification and role mapping to enterprise-grade services instead of relying solely on local accounts. By integrating with external authentication servers, you can align Crosswork Network Controller platform access with your organization's security standards. This integration also ensures scalable user management and supports regulatory compliance across teams.

Best practice for external server changes

Crosswork Network Controller supports configuration of up to 5 external authentication servers. When making changes to authentication server settings, observe the following recommendations:

- Perform all server additions, updates, or deletions in a single planned session to minimize user login disruptions.

- Ensure you have appropriate permissions before attempting to configure or delete external authentication servers.
- Wait a few minutes between consecutive changes to AAA server settings to avoid causing authentication errors or external login failures.
- Give write permission for remote authentication server APIs only to users who are authorized to manage or delete external authentication servers.
- After updating external server configuration in geo-redundant deployments, restart any standby appliance services as instructed by the documentation.
- Remember that changes to external authentication servers immediately affect all new user logins.

Configure TACACS+ servers

Add, update, or remove TACACS+ authentication servers to control user and device authentication in Crosswork Network Controller.

Crosswork Network Controller supports authentication of users via TACACS+ servers. You can integrate Crosswork with a standalone TACACS+ server (such as open TACACS+) or with an application like Cisco ISE (Identity Services Engine). Integrating with TACACS+ servers helps centralize and control access to network resources.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see *<xref to Create Device Access Group>*
- In the TACACS+ server (standalone or Cisco ISE), configure required parameters such as user role, device access group attribute, shared secret format, and shared secret value before adding the server to Crosswork Network Controller.
- For details on configuring Cisco ISE, refer to the latest Cisco Identity Services Engine Administrator Guide.

Follow these steps to configure TACACS+ servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **TACACS+** .

Step 2 To add a new TACACS+ server: Click  , enter required details (see TACACS+ field descriptions, on page 3), and click **Add**.

Step 3 To edit an existing TACACS+ server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a TACACS+ server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

TACACS+ authentication servers are added, updated, or removed as configured. Crosswork uses these servers for user and device authentication.

What to do next

Test user authentication with the updated TACACS+ server settings to confirm successful configuration.

TACACS+ field descriptions

The table lists the key fields required when configuring a TACACS+ server in Crosswork Network Controller.

Table 1: TACACS+ field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS name is supported.
Port	The default TACACS+ port number is 49.
Shared secret format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active TACACS+ server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the TACACS+ server.
Service	Enter the value of the service you are attempting to gain access to. This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter any value; do not leave the field blank. The service field is an attribute that tells the TACACS+ server what type of network service the user is trying to access. It allows the TACACS+ server to distinguish between different types of access, such as: • **Login access** (e.g., device CLI, SSH, console) • **Network access** (e.g., PPP, SLIP) For example, the "`raccess`" value is a service type used in the service field of an authorization request. It stands for **Remote Access** and is typically used when a user is requesting remote administrative access.

Field	Description
Policy ID	Enter the user role that you created in the TACACS+ server. The **Policy ID** is a unique key used by the TACACS+ server to identify and retrieve the user role assigned to an authenticated user. This value must exactly match the user role you configured on the TACACS+ server. In Crosswork Network Controller, this field corresponds to the *policy_id*. **Note** If you try to login to Crosswork Network Controller as a TACACS+ user before creating the required user role, you will get the error message: `"Key not authorized: no matching policy"`. If this occurs, close the browser. Login as a local admin user and create the missing user roles in the TACACS+ server, and login back to Crosswork using the TACACS+ user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the (ISE/Standalone) TACACS+ server attributes. These values can be one or more comma-separated entries. In a TACACS+ context, the Device Access Group attribute is typically a custom or authorization attribute that the TACACS+ server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy id to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for TACACS+: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Example

In this scenario, the TACACS+ parameters are configured in Cisco ISE.

- **Device Access Group** has already been created in Crosswork for AAA operation access.
- Relevant TACACS+ parameters configured in Cisco ISE:
  - **User profile**: `role0` (referenced in the **Policy Id** field)
  - **Device Access Group attribute**: `DAG-CONFIGURE`
  - **Shared secret format**: `ASCII`

Figure 1: Configure TACACS+ profile attributes in Cisco ISE

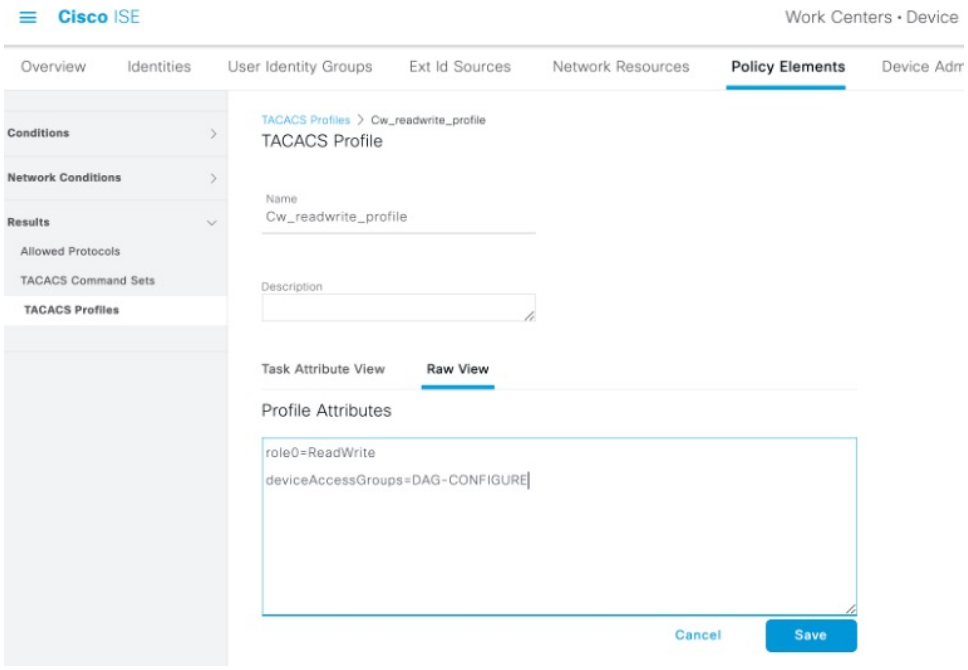
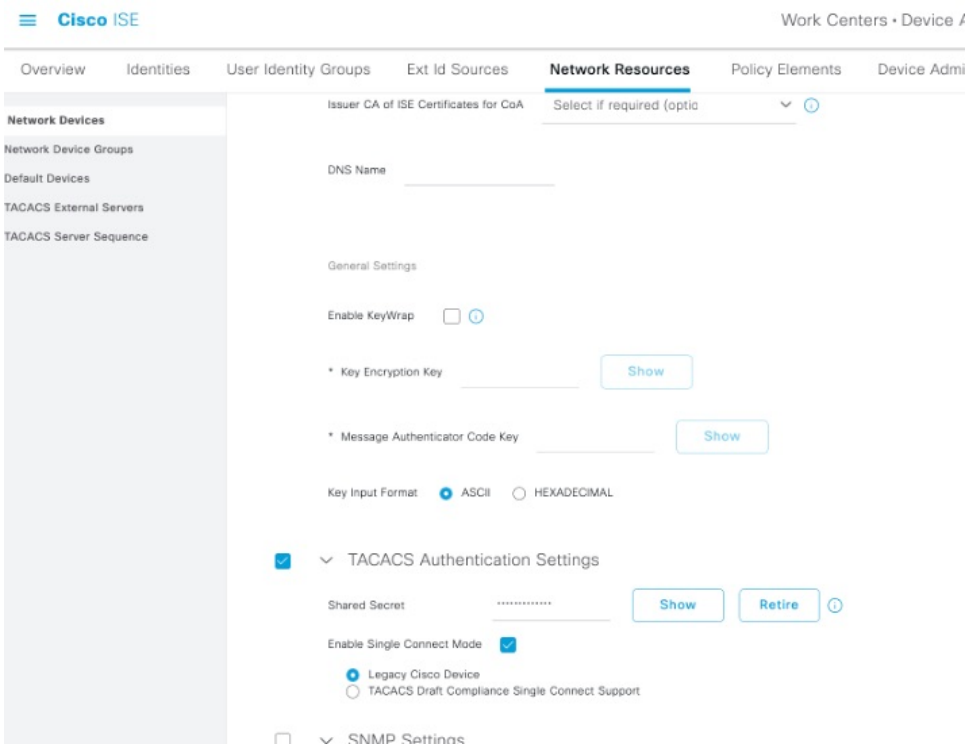
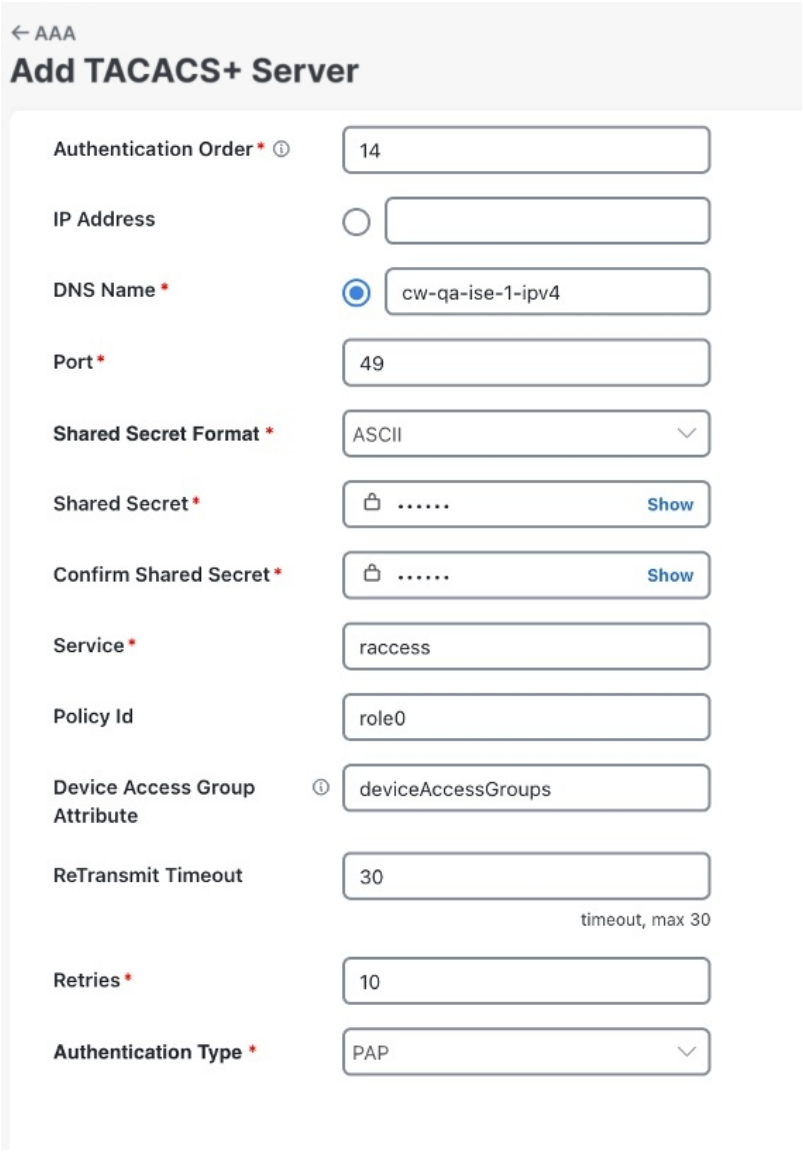


Figure 2: Configure TACACS+ authentication settings in Cisco ISE



Now, the TACACS+ server is added in Crosswork Network Controller UI:

Figure 3: Add TACACS+ server



API payload example

```
{
  "tacacs":{
    "tacacs_servers":[
    {
      "priority":10,
      "host":"cw-qa-ise-1-ipv4",
      "dnsName":"",
      "port":49,
      "secretFormat":"ascii",
      "secret":"sample",
      "service":"raccess",
      "policy-id": "role0",
```

```
      "virtualDomain":"deviceAccessGroups"
      "timeout":30,
      "retries":10,
      "authType":"pap",
    }
    ]
  }
}
```

Parameter mapping reference

```
Mapping reference:
-----------------------------------------------------------------------------------------------------------
Crosswork Network Controller                          CISCO ISE
VALUE
-----------------------------------------------------------------------------------------------------------
Device Access Group Attribute=deviceAccessGroups    deviceAccessGroups=DAG-CONFIGURE
DAG-CONFIGURE
PolicyId=role0                                      role0=ReadWrite
ReadWrite
```

Configure LDAP servers

Manage authentication connections by adding, editing, or deleting LDAP servers used for user authentication in Crosswork Network Controller.

Lightweight Directory Access Protocol (LDAP) servers, including OpenLDAP, Active Directory, and secure LDAP, are used to authenticate users for network management. Crosswork Network Controller can use these servers to centralize directory management and enforce access policies. Secure LDAP requires a certificate to enable encrypted communication.

Crosswork Network Controller supports two LDAP authentication modes:

- LDAP without Device Access Groups — LDAP returns a user-role attribute only.
- LDAP with Device Access Groups — LDAP returns both a user-role attribute and a device access group attribute. Crosswork Network Controller maps these values to configured roles and Device Access Groups.

LDAP attribute names shown in examples are for illustration only. Actual attribute names depend on your LDAP directory schema.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see Create Device Access Groups.
- Configure necessary parameters (such as bind DN, policy base DN, policy ID, and device access group attribute) on your LDAP server.
- For secure LDAP, add a "Secure LDAP Communication" certificate before proceeding. For details, see Add a new certificate.
- Ensure your LDAP server is already configured to return the required attributes (role and, if applicable, device access group) before setting up LDAP in Crosswork Network Controller.

- LDAP attribute names vary across deployments; the attribute names shown in examples (such as **sAMAccountName**) come from an engineering test environment and may not exist in your LDAP setup.
- DN values shown in this guide (such as `OU=ouUsers1`, `dc=DSEENIVA`, etc.) reflect the example LDAP directory structure. Use DN values from your own LDAP environment.
- The device access group attribute returned by LDAP must match the configured Device Access Group name in Crosswork Network Controller.

Follow these steps to configure LDAP servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **LDAP** .

Step 2 To add a new LDAP server: Click  , enter required details (see TACACS+ field descriptions, on page 3), and click **Add**.

Step 3 To edit an existing LDAP server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a LDAP server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

LDAP authentication servers are added, updated, or removed, and the changes are applied to authentication services in Crosswork Network Controller.

What to do next

Confirm the server is correctly listed and test user authentication if applicable.

LDAP field descriptions

The table lists the key fields that are required when you configure an LDAP server in Crosswork Network Controller.

Table 2: LDAP field descriptions

Field	Description
Authentication order	Defines the priority used when processing authentication requests. Accepts values from **10 to 99**; values below 10 are reserved for system use. The default value is **10**.
Name	A label used to identify the LDAP handler.
IP address/host name	The IP address or fully qualified hostname of the LDAP server.

Field	Description
Secure connection	Enables SSL-based LDAP communication. When selected, you must choose a **Secure LDAP Communication** certificate from the drop-down list. This field is disabled by default. **Note** The certificate must already exist in the Certificate Management screen before enabling secure LDAP.
Port	Specifies the port used to connect to the LDAP server. The default LDAP port is **389**. When secure LDAP is enabled, the default port is **636**.
Bind DN	The distinguished name (DN) used by Crosswork Network Controller to bind to the LDAP server for authentication queries.
Bind credential / Confirm bind credential	The username and password used to authenticate the Bind DN with the LDAP server.
Base DN	The starting point in the LDAP directory tree where Crosswork performs its user search operations.
User filter	The LDAP search filter used to locate user entries within the Base DN.
DN format	Specifies how user names are represented within the Base DN. This determines how Crosswork constructs the full DN for authentication queries.
Principal attribute ID	The attribute in the LDAP user profile that stores the user identifier (UID).
Policy base DN	The directory location used for role lookup and role mapping.
Policy map attribute	Identifies the attribute in the Policy base DN used to map a user to a specific role. This corresponds to the **userFilter** attribute on the LDAP server.
Policy ID	Specifies the role value returned by LDAP for the authenticated user. This value must match a corresponding user role configured on the LDAP server. In Crosswork Network Controller, this field maps to **policy_id**. **Note** If a user logs into Crosswork Network Controller before the required role exists on the LDAP server, authentication fails with: *"Login failed, policy not found. Please contact the Network Administrator for assistance."* Ensure LDAP roles are created before adding the LDAP server configuration in Crosswork Network Controller.
Device access group attribute	Specifies the LDAP attribute used to identify the user's device access group. This may include one or more comma-separated values. In LDAP environments, this attribute is typically a custom authorization value returned to the client. The returned value must correspond to an existing Device Access Group in Crosswork.
Connection timeout	Time (in seconds) allowed for LDAP operations to complete. The maximum allowed value is **30 seconds**.

LDAP example

This example shows parameters used for secure LDAP configuration. A Device Access Group named `"ALL-ACCESS"` is already configured in Crosswork Network Controller and referenced in LDAP.

Key points from the LDAP server configuration:

- The user role is **ldapa-user1**, part of the **ldapAdmin** group.
- The username is **DSEENIVA**.
- The policy ID returned by LDAP is **sAMAccountName**.
- `ldapUrl` contains the server hostname and port.
- In `ldap_attr_server` fields:
  - `baseDN` corresponds to **Policy base DN**.
  - `userFilter` corresponds to **Policy map attribute**.
- Device access group is returned via: `Description='ALL-ACCESS'`.

API payload example

DN samples used in the example (such as `dc=DSEENIVA,dc=COM` or `OU=ouUsers1`) reflect only the example directory's structure. Use the DN values from your LDAP environment.

Attention The following example is the LDAP server's response used during testing. It is not the CNC API request payload. Attribute names and DN structure are specific to that test environment. Use your own directory's attribute names and values when configuring LDAP.

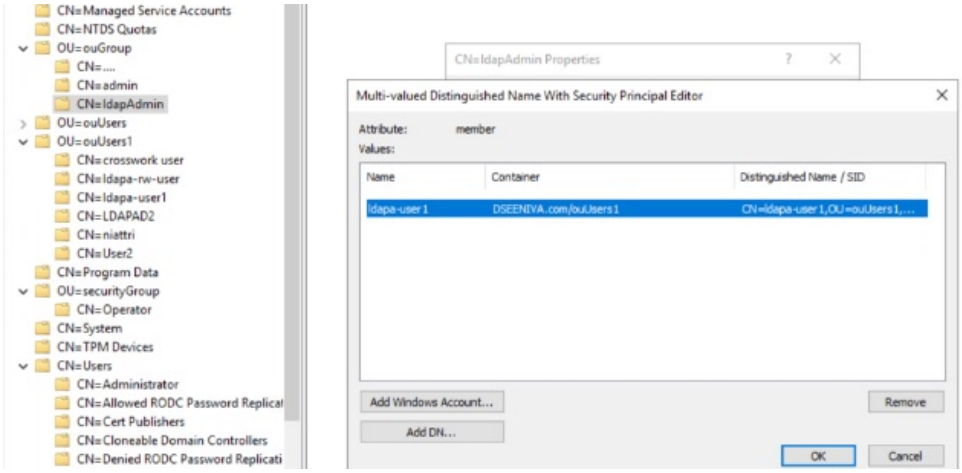
```
json:Y

{   "ldap": {
    "ldap_servers": {
      "ldap_server": [{
          "type": "DIRECT",
          "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "connectionStrategy": "",
          "useSsl": false,
          "useStartTls": false,
          "connectTimeout": 10,
          "baseDn": "OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "userFilter": "cn={user}",
          "subtreeSearch": true,
          "usePasswordPolicy": false,
          "dnFormat": "cn=%s,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "principalAttributeId": "cn",
          "policyId": "Description",
          "minPoolSize": 1,
          "maxPoolSize": 1,
          "validateOnCheckout": false,
          "validatePeriodically": true,
          "validatePeriod": 600,
          "idleTime": 5000,
          "prunePeriod": 5000,
          "blockWaitTime": 5000,
```

```
      "providerClass": "org.ldaptive.provider.unboundid.UnboundIDProvider",
      "allowMultipleDns": false,
      "order": 16,
      "trustStore": "ldaps",
      "name": "ldapsecure",
      "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
      "bindCredential": "<>"
    }
  ],
  "ldap_attr_servers": {
    "ldap_attr_server": [
      {
        "baseDn": "OU=ouGroup,dc=DSEENIVA,dc=COM",
        "trustStore": "ldaps",
        "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
        "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
        "bindCredential": "<>",
        "userFilter": "member=cn={user},OU=ouUsers1,dc=DSEENIVA,dc=COM",
        "failFast": false,
        "attributes": {
        "policy_id":"sAMAccountName"
        }}]}}}
```

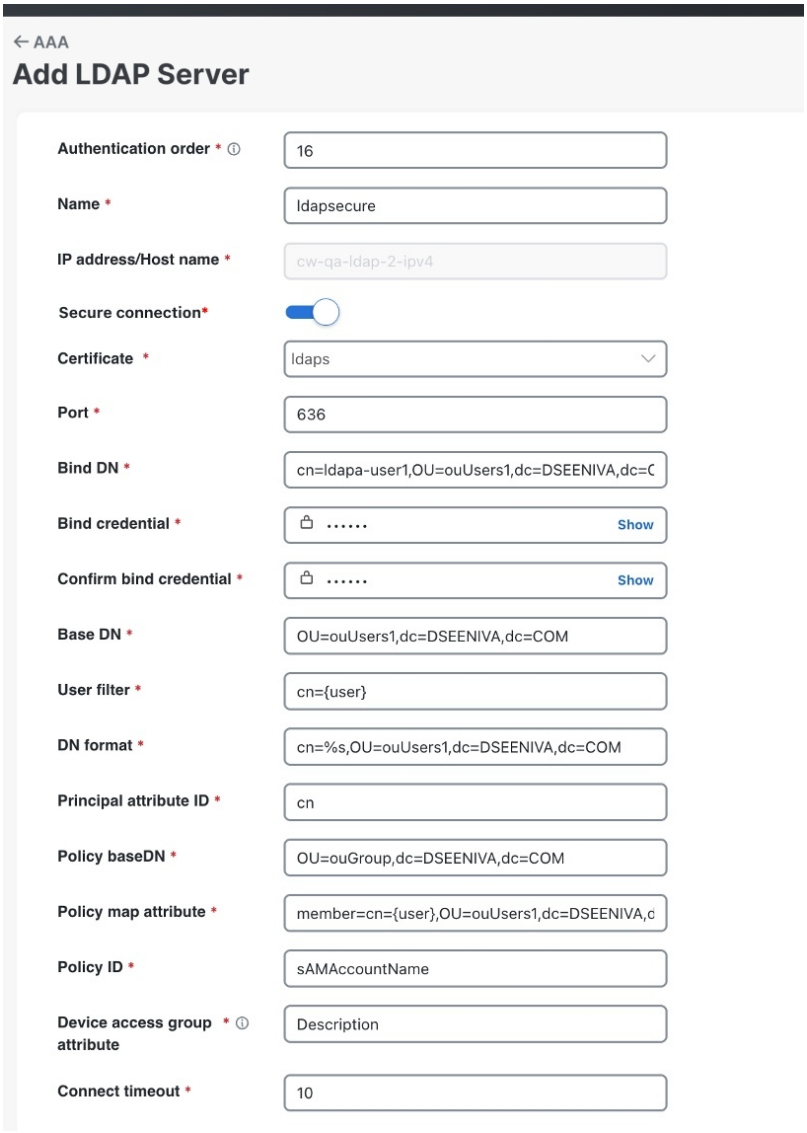
The user group and user role mapping configured in LDAP server:

Figure 4: Map user group and user role in LDAP server



Here is the corresponding LDAP configuration in the Crosswork Network Controller UI:

Figure 5: Add LDAP server



Configure RADIUS servers

Add, edit, or delete RADIUS servers to enable centralized user authentication and authorization in Cisco Crosswork.

Crosswork uses RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can integrate Crosswork with applications such as Cisco Identity Services Engine (ISE) for RADIUS-based authentication.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see *<xref to Create Device Access Group>*

- In the RADIUS server (standalone or Cisco ISE), configure required parameters such as user role, device access group attribute, shared secret format, and shared secret value before adding the server to Crosswork Network Controller.
- For details on configuring Cisco ISE, refer to the latest Cisco Identity Services Engine Administrator Guide.

Follow these steps to configure RADIUS servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **RADIUS** .

Step 2 To add a new RADIUS server: Click  , enter required details (see RADIUS field descriptions, on page 13), and click **Add**.

Step 3 To edit an existing RADIUS server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a RADIUS server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

RADIUS authentication servers are added, updated, or removed as configured. Crosswork uses these servers for user and device authentication.

What to do next

Test user authentication with the updated RADIUS server settings to confirm successful configuration.

RADIUS field descriptions

The following table describes the key fields required when configuring a RADIUS server in Crosswork Network Controller:

Table 3: RADIUS field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the RADIUS server (if IP address is selected).
DNS name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.

Field	Description
Shared secret / Confirm shared secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the RADIUS server.
Service	Enter the value of the service you are attempting to gain access to. The service field is an attribute that tells the RADIUS server what type of network service the user is trying to access. It allows the RADIUS server to distinguish between different types of access, such as: • **Login access** (e.g., device CLI, SSH, console) • **Network access** (e.g., PPP, SLIP) For example, the "`raccess`" value is a service type used in the service field of an authorization request. It stands for **Remote Access** and is typically used when a user is requesting remote administrative access.
Policy ID	Enter the user role that you created in the RADIUS server. The **Policy ID** is a unique key used by the RADIUS server to identify and retrieve the user role assigned to an authenticated user. This value must exactly match the user role you configured on the RADIUS server. In Crosswork Network Controller, this field corresponds to the *policy_id*. **Note** If you try to login to Crosswork Network Controller as a RADIUS user before creating the required user role, you will get the error message: "`Key not authorized: no matching policy`". If this occurs, close the browser. Login as a local admin user and create the missing user roles in the RADIUS server, and login back to Crosswork using the RADIUS user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the RADIUS server attributes. These values can be one or more comma-separated entries. In a RADIUS context, the Device Access Group attribute is typically a custom or authorization attribute that the RADIUS server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy id to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.

Field	Description
Authentication type	Select the authentication type for RADIUS: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Configure AAA settings

Control user authentication, authorization, and accounting on the system by configuring AAA settings to enforce security policies and manage user sessions.

Users with relevant AAA permissions can configure the AAA settings.

Configure these settings when you need to establish or update how users are authenticated, what resources they can access, and how their activities are tracked. Proper AAA settings help safeguard network resources and ensure compliance with organizational access policies.

Before you begin

- Ensure you have administrator permissions or equivalent AAA configuration rights.
- Review your organization's authentication and password policy requirements.
- Gather information about external authentication servers (if applicable).
- Notify affected users of possible session interruptions during configuration changes.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **Settings** .

Step 2 Select the relevant setting for **Fallback to local**. By default, Crosswork Network Controller prefers external authentication servers over local database authentication.

Note
Admin users are always authenticated locally.

Step 3 Under **Browser session timeout**, select the relevant value for the **Log out inactive users after** field. Any user who remains idle beyond the specified limit will be automatically logged out.

This timeout is enforced by the system and applies even if the user closes the browser tab without explicitly logging out. If no activity (token usage) is detected after the tab is closed, the session expires after the configured timeout. For example, with a 10-minute timeout, if a user closes the browser tab after 5 minutes of activity, the user must log in again if they return after 10 minutes.

Note

- The default timeout value is 30 minutes.
- Changes to the timeout value take effect immediately, including for active sessions.
- Session termination can take upto a minute more than the configured timeout due to backend scheduling.
- This setting applies only to browser-based UI sessions. API-based sessions continue to follow the existing 8-hour validity behavior.

Step 4 Under **Parallel session**, enter relevant values for the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note
Crosswork Network Controller supports between 5 to 200 parallel session for concurrent users. If the number of parallel sessions are exceeded, an error is displayed while logging in to Crosswork Network Controller .

Note
Crosswork Network Controller supports 50 simultaneous NBI sessions up to 400 sessions.

Step 5 Under **Source IP**, enable auditing of user source IP addresses.

a) Select the **Enable source IP for auditing** checkbox to log the user's source IP address for auditing and accounting. This option is disabled by default.
b) Log out, wait a few minutes, then log back in. This pause ensures the change is applied and the actual client IP address is accurately captured.

   During this transition, audit logs may temporarily display the Crosswork node IP instead of the client IP. The correct client IP will appear in new audit log entries created after you log in again. Previous log entries will continue to show the node IP. Once enabled and you have logged in again, the **Source IP** column will appear on both the **Audit Log** and **Active sessions** pages.

Step 6 Select the relevant settings for the **Local password policy**. Certain password settings are enabled by default and cannot be disabled (for example, Change password on first login).

Note
Any changes in the password policy is enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

Note
Local password policy allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of Crosswork Network Controller , and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

Enable single sign-on

Enable single sign-on (SSO) so users can access multiple related applications with a single set of credentials, streamlining authentication and simplifying navigation between service providers.

Single sign-on (SSO) is an authentication method that lets users log in once and access multiple independent systems without reentering credentials. Crosswork Network Controller acts as an Identity Provider (IdP) and

supports SSO integration for service provider applications. You can enable SSO for users authenticated via TACACS+, LDAP, and RADIUS. When SSO is configured, users benefit from seamless access and improved security management.

Crosswork Network Controller also supports SSO cross-launch, so users can move easily between Crosswork Network Controller and integrated applications. Once configured, the URL can be launched using the launch icon ( ) located at the top right corner of the window.

Note that the Crosswork Network Controller login page is not shown if the Central Authentication Service (CAS) pod is restarting or offline.

Attention

- When Crosswork Network Controller's CAS pod is restarting or not running, the login page is not available.
- The SSO URL from the Identity Provider (IdP) is *https://<IP>:30603/crosswork/sso/idp/profile/SAML2/Redirect/SSO*, where <IP> represents the Crosswork Network Controller's IP address or hostname.

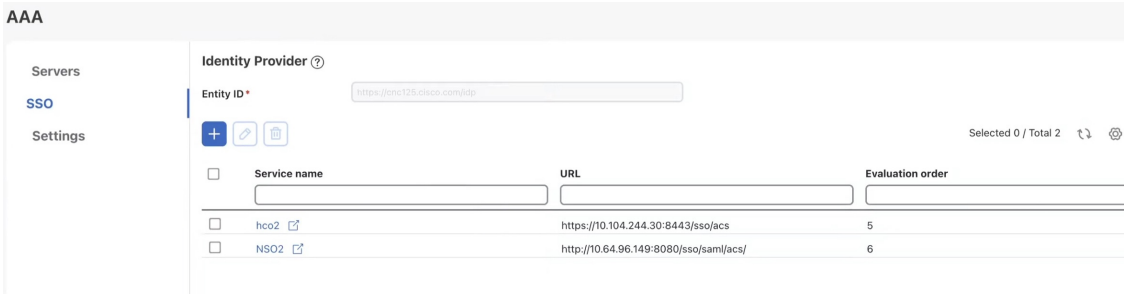
Before you begin

- Select **Enable source IP for auditing** check box on the **Administration** > **AAA** > **Settings** page.
- Ensure you have the latest service provider metadata to integrate with Crosswork Network Controller SSO.
- Confirm that network connectivity exists between Crosswork Network Controller (IdP) and each service provider application.
- Verify the CAS pod is running and stable.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO** . The **Identity Provider** window appears. You can add, edit or delete SSO providers here.

Figure 6: Identity Provider window



Step 2 To add a new service provider:

a) Click the icon.

b) In the **Service Provider** window, enter the values in the following fields:

- **Name**: Specify the entity name.
- **Evaluation order**: Assign a unique number for service definition priority.
- **Metadata**: Provide or browse to the SAML metadata XML document for the service provider.

Note
If you supply a URL, the **Service name** entry becomes a hyperlink for cross-launch.

c) Click **Add** to confirm.

Step 3 Click **Save all changes**. When prompted, confirm by clicking **Save changes**.

Note
Saving changes may require restarting the server for updates to take effect.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Crosswork Network Controller server. After providing the Crosswork credentials, the service provider application logs in automatically. For all the subsequent application logins, you do not have to enter any authentication details.

Step 4 To edit a service provider:

a) Select the check box next to the service provider, then click the icon.
b) Update evaluation order or metadata information as needed.
c) Click **Update** to apply changes.

Step 5 To delete a service provider:

a) Select the check box next to the service provider, then click the icon.
b) Click **Delete** to confirm removal.

Single sign-on is enabled for selected service provider applications. Users can authenticate once via Crosswork Network Controller and seamlessly access associated applications without reentering authentication factors.

What to do next

- If Crosswork Network Controller is reinstalled or migrated, update the Identity Provider (IdP) metadata in all service provider applications to avoid authentication errors due to metadata mismatch.
- For first-time users, ensure password change is completed before attempting to log in with a different username. To reset an incomplete session, an administrator must terminate it.