Realms and Identity Policies

A *realm* consists of one or more LDAP or Microsoft Active Directory servers that share the same credentials. You must configure a realm if you want to perform user and user group queries, user access control, or to configure a User Agent, ISE/ISE-PIC, or captive portal. After configuring one or more realms, you can configure an identity policy.

An *identity policy* associates traffic on your network with an authoritative identity source and a realm. After configuring your identity policy, you can associate it with an access control policy and deploy the access control policy to your device.

Realm Fundamentals

License: Any

Realms establish connections between the ASA FirePOWER module and the servers targeted for monitoring. They specify the connection settings and authentication filter settings for the server. Realms can:

- specify the users and user groups whose activity you want to monitor.
- allow you to query the server for user metadata on authoritative users.

You can add multiple servers as directories within a realm, but they must share the same basic realm information. The directories within a realm must be exclusively LDAP or exclusively AD servers. After you enable a realm, your saved changes take effect next time the ASA FirePOWER module queries the server.

To perform user awareness, you must configure a realm for any of the supported server types. The module uses these connections to query the servers for data associated with POP3 and IMAP users. The module uses the email addresses in POP3 and IMAP logins to correlate with LDAP users on an Active Directory, OpenLDAP, or Oracle Directory Server Enterprise Edition server. For example, if a device detects a POP3 login for a user with the same email address as an LDAP user, the module associates the LDAP user's metadata with that user.

To perform user access control, you can configure the following:

- a realm for an AD server configured for either a User Agent or ISE/ISE-PIC device.

Note Configuring a realm is optional if you plan to configure SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions.

- a realm for an Oracle or OpenLDAP server configured for captive portal.

If you configure a realm to download users (for user awareness or user control), the ASA FirePOWER module regularly queries the server to obtain metadata for new and updated users whose activity was detected since the last query.

User activity data is stored in the user activity database and user identity data is stored in the users database. The maximum number of users you can store and use in access control depends on your device model. When choosing which users and groups to include, make sure the total number of users is less than your model limit. If your access control parameters are too broad, the ASA FirePOWER module obtains information on as many users as it can and reports the number of users it failed to retrieve in the task queue.

Note If you remove a user that has been detected by the module from your LDAP servers, the ASA FirePOWER module does not remove that user from its users database; you must manually delete it. However, your LDAP changes are reflected in access control rules when the ASA FirePOWER module next updates its list of authoritative users.

Supported Servers for Realms

License: Any

You can configure realms to connect to the following types of servers, providing they have TCP/IP access from the ASA FirePOWER module:

Table 32-1 Supported Servers for Realms

Server Type	Supported for user awareness data retrieval?	Supported for User Agent data retrieval?	Supported for ISE/ISE-PIC data retrieval?	Supported for captive portal data retrieval?
Microsoft Active Directory on Windows Server 2003, Windows Server 2008, and Windows Server 2012	Yes	Yes	Yes	Yes, except Windows Server 2003 if you are using NTLM captive portal
Oracle Directory Server Enterprise Edition 7.0 on Windows Server 2003 and Windows Server 2008	Yes	No	No	Yes
OpenLDAP on Linux	Yes	No	No	Yes

Note the following about your server group configurations:

- If you want to perform user control on user groups or on users within groups, you must configure user groups on the server. The ASA FirePOWER module cannot perform user group control if the server organizes the users in basic object hierarchy.

  Cisco recommends that you limit the size of your LDAP or AD server groups to contain a maximum of 1500 users. Configuring realms to include or exclude oversized groups, or creating access control rules that target oversized user groups may result in performance issues.
- By default, AD servers limit the number of users they report from secondary groups. You must customize this limit so that all of the users in your secondary groups are reported to the ASA FirePOWER module.

Supported Server Field Names

License: Any

The servers in your realms must use the field names listed in the following table in order for the ASA FirePOWER module to retrieve user metadata the servers. If the field names are incorrect on your server, the ASA FirePOWER module cannot populate its database with the information in that field.

Table 32-2 Mapping Server Fields to ASA FirePOWER Fields

Metadata	ASA FirePOWER module	Active Directory	Oracle Directory Server	OpenLDAP
LDAP user name	Username	samaccountname	cn uid	cn uid
first name	First Name	givenname	givenname	givenname
last name	Last Name	sn	sn	sn
email address	Email	mail userprincipalname (if mail has no value)	mail	mail
department	Department	department distinguishedname (if department has novalue)	department	ou
telephone number	Phone	telephonenumber	n/a	telephonenumber

Troubleshooting Issues with Realms

License: Any

If you notice unexpected server connection behavior, consider tuning your realm configuration, device settings, or server settings.

User timeouts are occurring at unexpected times

If you notice the system performing user timeouts at unexpected intervals, confirm that the time on your User Agent or ISE/ISE-PIC device is synchronized with the time on the ASA FirePOWER module. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.

Users are not included or excluded as specified in your realm configuration

If you configure a realm for an Active Directory server that includes or excludes users who are members of a secondary group on your Active Directory server, your server may be limiting the number of users it reports.

By default, Active Directory servers limit the number of users they report from secondary groups. You must customize this limit so that all of the users in your secondary groups are reported to the ASA FirePOWER module.

User download is slow

If you notice that user download is slow, confirm that your LDAP and AD server groups contain a maximum of 1500 users. Configuring realms to include or exclude oversized user groups may result in performance issues.

Identity Policy Fundamentals

License: Any

Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

You must fully configure the realms and authentication methods you plan to use before you can invoke them in your identity rules:

- You configure realms outside of your identity policy, at **Configuration > ASA FirePOWER Configuration > Integration > Realms**.
- You configure the passive authentication identity sources, the User Agent and ISE/ISE-PIC, at **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources**.
- You configure the active authentication identity source, captive portal, within the identity policy.

After you configure one or more identity policies, you must invoke one identity policy in your access control policy. When traffic on your network matches the conditions in your identity rule and the authentication method is passive or active, the module associates the traffic with the specified realm and authenticates the users in the traffic using the specified identity source.

If you do not configure an identity policy, the module does not perform user authentication.

Creating a Realm

License: Control

To create a realm:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration**.

Step 2 Click **Realms**.

Step 3 Click **New Realm**.

Step 4 Configure basic realm information as described in Configuring Basic Realm Information, page 32-7.

Step 5 Configure directories as described in Configuring a Realm Directory, page 32-7.

Step 6 Configure user and user group download (required for access control) as described in Configuring Automatic User Download, page 32-8.

Step 7 Save the realm settings.

Step 8 Optionally, edit the realm and modify the default User Session Timeout settings as described in Configuring Realm User Session Timeouts, page 32-8.

Step 9 Save the realm settings.

What to Do Next

- Enable the realm as described in Enabling or Disabling a Realm, page 32-18.
- Optionally, monitor the task status; see the Task Status page (**Monitoring > ASA FirePOWER Monitoring > Task Status**).

Realm Fields

License: Any

The following fields are used to configure a realm.

Realm Configuration Fields

AD Primary Domain

For AD realms only, the domain for the Active Directory server where users should be authenticated.

AD Join Username and AD Join Password

For AD realms intended for Kerberos captive portal active authentication, the distinguished username and password for a user with appropriate rights to join clients to the domain.

If you select Kerberos (or HTTP Negotiate, if you want Kerberos as an option) as the **Authentication Type** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** in order to perform Kerberos captive portal authentication.

Description

An optional description for the realm.

Directory Username and Directory Password

The distinguished username and password for a user with appropriate rights to the user information you want to retrieve.

Base DN

The directory tree on the server where the ASA FirePOWER module should begin searching for user data.

Typically, the base DN has a basic structure indicating the company domain and operational unit. For example, the Security organization of the Example company might have a base DN of ou=security,dc=example,dc=com.

Group DN

The directory tree on the server where the ASA FirePOWER module should search for users with the group attribute.

Group Attribute

The group attribute for the server: Member, Unique Member, or Custom.

Name

A unique name for the realm.

Type

The type of realm, AD or LDAP.

User Session Timeout: Authenticated Users

The maximum amount of time, in minutes, before a user's session is timed out.

If a user was passively authenticated and their session times out, they are identified as Unknown and their current session is allowed or blocked depending on their access control rule settings. The module re-identifies the user the next time they log in.

If a user was actively authenticated (captive portal) and their session times out, they are prompted to re-authenticate.

User Session Timeout: Failed Authentication Users

The amount of time, in minutes, after a failed active authentication attempt that a user's session is timed out. When a user fails to authenticate and their session times out, they are prompted to re-authenticate.

User Session Timeout: Guest Users

The maximum amount of time, in minutes, before an actively authenticated (captive portal) guest user's session is timed out. When their session times out, they are prompted to re-authenticate.

Realm Directory Fields

These settings apply to individual servers (directories) within a realm.

Encryption

The encryption method you want to use for the server connection. If you specify an Encryption method, you must specify a host name in this field.

Hostname / IP Address

The hostname or IP address for the server.

Port

The port you want to use for the server connection.

SSL Certificate

The SSL certificate you want to use for authentication to the server. You must configure the **Encryption** type in order to use an SSL certificate.

If you are using a certificate to authenticate, the name of the server in the certificate must match the server **Hostname / IP Address**. For example, if you use 10.10.10.250 as the IP address but computer1.example.com in the certificate, the connection fails.

User Download Fields

Download for access control

Selecting this check box configures the automatic download of user data. You can use the data for user awareness and, in some cases, user access control.

Use the **Begin automatic download at and Repeat every drop-down** menus to configure the download frequency.

Configuring Basic Realm Information

License: Control

To configure basic realm information:

Step 1 On the Add New Realm page, type a **Name** and, optionally, a **Description**.

Step 2 Select a **Type** from the drop-down list.

Step 3 If you are configuring an AD realm, enter an **AD Primary Domain**.

Step 4 If you are configuring an AD realm intended for Kerberos captive portal active authentication, enter a distinguished **AD Join Username** and **AD Join Password** for a user with appropriate rights to join clients to the domain.

Step 5 Enter a distinguished **Directory Username** and **Directory Password** for a user with appropriate rights to the user information you want to retrieve.

Step 6 Enter a **Base DN** for the directory.

Step 7 Enter a **Group DN** for the directory.

Step 8 Optionally, select a **Group Attribute** from the drop-down list.

Step 9 Click **OK**.

What to Do Next

- Configure the realm directory as described in Configuring a Realm Directory, page 32-7.

Configuring a Realm Directory

License: Control

To configure a realm directory:

Step 1 On the Directory tab, click **Add Directory**.

Step 2 Enter the Hostname / IP Address and Port for the server.

Step 3 Select an Encryption Mode.

Step 4 Optionally, select an SSL Certificate from the drop-down list. Note that you can click the add icon ( ) to create an object on the fly.

Step 5 If you want to test the connection, click **Test**.

Step 6 Click **OK**.

What to Do Next

- Optionally, configure automatic user download as described in Configuring Automatic User Download, page 32-8.

Configuring Automatic User Download

License: Control

If you do not specify any groups to include, the ASA FirePOWER module retrieves user data for all the groups that match the parameters you provided. For performance reasons, Cisco recommends that you explicitly include only the groups that represent the users you want to use in access control.

To configure automatic user download:

Step 1 On the User Download tab, select the **Download users and groups (required for user access control)** check box.

Step 2 Select a time to **Begin automatic download at** from the drop-down lists.

Step 3 Select a download interval from the **Repeat Every** drop-down list.

Step 4 To include or exclude user groups from the download, select user groups from the **Available Groups** column and click **Add to Include** or **Add to Exclude**.

Step 5 To include or exclude individual users, type the user into the field below Groups to Include or Groups to Exclude and click **Add**.

Note Excluding users from download prevents you from writing an access control rule with that user as a condition. Separate multiple users with commas. You can also use an asterisk (*) as a wildcard character in this field.

Configuring Realm User Session Timeouts

License: Control

Note If the module is performing user timeouts at unexpected intervals, confirm that the time on your User Agent or ISE/ISE-PIC device is synchronized with the time on the ASA FirePOWER module.

To configure realm user session timeouts:

Step 1 Select the **Realm Configuration** tab.

Step 2 Enter user session timeout values for **Authenticated Users**, **Failed Authentication Users**, and **Guest Users**.

Step 3 Click **Save** or continue editing the realm.

Configuring an Identity Policy

License: Control

Before You Begin

- Create and enable one or more realms as described in Creating a Realm, page 32-4.

To configure an Identity Policy:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**.

Step 2 Type a **Name** and, optionally, a **Description**.

Step 3 If you want to add a rule to the policy, click Add Rule as described in Creating an Identity Rule, page 32-12

Step 4 If you want to add a rule category, click Add Category as described in Adding an Identity Rule Category, page 32-19

Step 5 If you want to configure active authentication using captive portal, click Active Authentication as described in Configuring Captive Portal (Active Authentication), page 32-10.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Captive Portal (Active Authentication) Fields

License: Any

Use the following fields to configure captive portal.

Server Certificate

The server certificate presented by the captive portal daemon.

Port

The port number you want to use for the captive portal connection. The port number in this field must match the port number you configured on the ASA FirePOWER device using the `captive-portal` CLI command.

Maximum login attempts

The maximum allowed number of failed login attempts before the module denies a user's login request.

Active Authentication Response Page

The system-provided or custom HTTP response page you want to display to captive portal users. After you select an Active Authentication Response page in your identity policy active authentication settings, you must also configure one or more identity rules with HTTP Response Page as the Authentication Type.

The system-provided HTTP response page includes Username and Password fields, as well as a **Login as guest** button to allow users to access the network as guests. If you want to display a single login method, configure a custom HTTP response page.

Configuring Captive Portal (Active Authentication)

License: Control

You can select either a system-provided or a custom HTTP response page to display to captive portal users. The system-provided HTTP response page includes Username and Password fields, as well as a **Login as guest** button to allow users to access the network as guests. If you want to display a single login method, configure a custom HTTP response page.

For more information about captive portal, see The Captive Portal Active Authentication Identity Source, page 33-7.

Before You Begin

- Confirm that your device manages one or more ASA FirePOWER devices in routed mode running Version 9.5(2) or later.
- Configure an access control rule to allow traffic destined for the port you plan to use for captive portal.
- If you want to perform active authentication via captive portal on HTTPS traffic, you must create SSL rules to decrypt the traffic originating from the users you want to authenticate using captive portal.
- If you want to decrypt traffic in the captive portal connection, create an SSL rule to decrypt the traffic destined for the port you plan to use for captive portal.
- Use the `captive-portal` ASA CLI command to enable captive portal for active authentication and define the port as described in the *ASA Firewall Configuration Guide* (Version 9.5(2) or later): http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html.

To configure captive portal:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy** and edit an identity policy.

Step 2 Click **Active Authentication**.

Step 3 Select the appropriate **Server Certificate** from the drop-down list. Optionally, click the add icon ( ) to create an object on the fly.

Step 4 Type a **Port** and specify the **Maximum login attempts**.

Step 5 Optionally, to authenticate users through a HTTP response page, select an **Active Authentication Response Page**.

Step 6 Click **Save**.

Step 7 Configure an identity rule with **Active Authentication** as the **Action** as described in Creating an Identity Rule, page 32-12. If you selected a response page in step 5, you must also select HTTP Response Page as the **Authentication Type**.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Excluding Applications From Active Authentication

License: Control

You can select applications (identified by their HTTP User-Agent strings) and exempt them from captive portal (active authentication). This allows traffic from the selected applications to pass through the identity policy without authenticating.

To exclude applications from active authentication:

Step 1 On the **Realm & Settings** tab of the identity rule editor page, use Cisco-provided filters in the **Application Filters** list to narrow the list of applications you want to add to the filter.

- Click the arrow next to each filter type to expand and collapse the list.
- Right-click a filter type and click **Check All** or **Uncheck All**. Note that the list indicates how many filters you have selected of each type.
- To narrow the filters that appear, type a search string in the **Search by name** field; this is especially useful for categories and tags. To clear the search, click the clear icon ( ).
- To refresh the filters list and clear any selected filters, click the reload icon ( ).
- To clear all filters and search fields, click **Clear All Filters**.

Note The list displays 100 applications at a time.

Step 2 Select the applications that you want to add to the filter from the **Available Applications** list:

- Select **All apps matching the filter** to add all the applications that meet the constraints you specified in the previous step.
- To narrow the individual applications that appear, type a search string in the **Search by name** field. To clear the search, click the clear icon ( ).
- Use the paging icons at the bottom of the list to browse the list of individual available applications.
- To refresh the applications list and clear any selected applications, click the reload icon ( ).

Step 3 Add the selected applications to exclude from external authentication. You can click and drag, or you can click **Add to Rule**. The result is the combination of:

- the selected Application Filters

- either the selected individual Available Applications, or **All apps matching the filter**

What to Do Next

- Continue configuring the identity rule as described in Creating an Identity Rule, page 32-12.

Associating an Identity Policy with an Access Control Policy

License: Control

You can have one identity policy currently applied to an ASA FirePOWER module. You cannot apply an identity policy independently. You cannot delete an identity policy that has been applied or is currently applying.

To associate an Identity Policy with an Access Control Policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

Step 2 Select the **Advanced** tab.

Step 3 Click the edit icon ( ) next to Identity Policy Settings.

Step 4 Select an identity policy from the drop-down.

Step 5 Click **OK**.

Step 6 Click **Store ASA FirePOWER Changes** to save your changes.

Creating an Identity Rule

License: Control

To create an identity rule:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**.

Step 2 Click **Add Rule**.

Step 3 Configure basic identity rule information as described in Configuring Basic Identity Rule Information, page 32-14.

Step 4 Optionally, add a zone condition as described in Adding a Zone Condition to an Identity Rule, page 32-16.

Note If you are configuring the rule for captive portal and your captive portal device contains inline and routed interfaces, you must configure a zone condition to target only the routed interfaces on the device.

Step 5 Optionally, add a network or geolocation condition as described in Adding a Network or Geolocation Condition to an Identity Rule, page 32-15.

Step 6 Optionally, add a port condition as described in Adding a Port Condition to an Identity Rule, page 32-15.

Step 7 Associate the rule with a realm as described in Associating a Realm and Configuring Active Authentication Settings in an Identity Rule, page 32-16.

Step 8 Click **Add**.

Step 9 Click **Store ASA FirePOWER Changes**.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Identity Rule Fields

Use the following fields to configure identity rules.

Enabled

Selecting this option enables the identity rule in the identity policy. Deselecting this option disables the identity rule.

Action

The type of authentication you want to perform on the users in the specified **Realm**. You can select Passive Authentication (User Agent or ISE/ISE-PIC), Active Authentication (captive portal), or No Authentication. You must fully configure the authentication method, or identity source, before selecting it as the action in an identity rule.

Realm

The realm containing the users you want to perform the specified **Action** on. You must fully configure a realm before selecting it as the realm in an identity rule.

If you select Kerberos (or HTTP Negotiate, if you want Kerberos as an option) as the A**uthentication Type** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** in order to perform Kerberos captive portal authentication.

Use active authentication if passive authentication cannot identify user

Selecting this option authenticates users via active authentication if passive authentication fails to identify them. You must configure active authentication (captive portal) in order to select this option.

If you disable this option, users that passive authentication cannot identify are identified as Unknown. You must set the rule action to Passive Authentication in order to see this field.

Identify as Special Identities/Guest if authentication cannot identify user

Selecting this option identifies unknown users as **Special Identities/Guest** in all areas of the ASDM interface. You must set the rule action to Active Authentication or select **Use active authentication if passive authentication cannot identify user** in order to see this field.

Authentication Type

The method you want to use to perform active authentication. The selections vary depending on the type of realm, LDAP or AD:

– Select HTTP Basic if you want to authenticate users using an unencrypted HTTP Basic Authentication (BA) connection. Users log in to the network using their browser's default authentication popup window.

Most web browsers cache the credentials from HTTP Basic logins and use the credentials to seamlessly begin a new session after an old session times out.

– Select NTLM if you want to authenticate users using a NT LAN Manager (NTLM) connection. This selection is only available when you select an AD realm. Users log in to the network using their browser's default authentication popup window. If you select NTLM as your identity rule Authentication Type, you cannot use a 2003 Windows Server as your identity rule realm.

– Select Kerberos if you want to authenticate users using a Kerberos connection. This selection is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.

  The **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** in order to perform Kerberos captive portal authentication.

Note If you have DNS resolution configured and you create an identity rule to perform Kerberos (or HTTP Negotiate, if you want Kerberos as an option) captive portal, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the hostname you provided when configuring DNS. For ASA with FirePOWER Services devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.

– Select HTTP Negotiate to allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection. This selection is only available when you select an AD realm. Users log in to the network using their browser's default authentication popup window.

  The **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** in order to perform Kerberos captive portal authentication.

  If you are creating an identity rule to perform HTTP Negotiate captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the hostname of the captive portal device. The hostname of the device you are using for captive portal must match the host name you provided when configuring DNS.

– Select HTTP Response Page if you want to authenticate users using a ASA FirePOWER module-provided or custom HTTP response page. Users log in to the network using the response page you configure.

  The system-provided HTTP response page includes Username and Password fields, as well as a **Login as guest** button to allow users to access the network as guests. If you want to display a single login method, configure a custom HTTP response page.

  Users who log in as guests appear in the web interface with the username **Guest**, and their realm is the realm specified in the identity rule.

Configuring Basic Identity Rule Information

License: Control

To configure basic identity rule information:

Step 1 On the identity rule editor page, type a **Name**.

Step 2 Specify whether the rule is **Enabled**.

Step 3 To add the rule to a rule category, see Adding an Identity Rule Category, page 32-19.

Step 4 Select a rule **Action** from the drop-down list.

Step 5 Click **Add** or continue editing the rule.

Adding a Network or Geolocation Condition to an Identity Rule

License: Control

To add a network or geolocation condition to an Identity Rule:

Step 1 On the identity rule editor page, select the **Networks** tab.

Step 2 Find the networks you want to add from the **Available Networks**, as follows:

- To add a network object on the fly, which you can then add to the condition, click the add icon ( ) above the Available Networks list.
- To search for network or geolocation objects to add, select the appropriate tab, click the **Search by name or value** prompt above the **Available Networks** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.

Step 3 To select an object, click it. To select all objects, right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination**.

Step 5 Add any source or destination IP addresses or address blocks that you want to specify manually. Click the **Enter an IP address** prompt below the **Source Networks** or **Destination Networks** list; then type an IP address or address block and click **Add**.

Step 6 Click **Add** or continue editing the rule.

Adding a Port Condition to an Identity Rule

License: Control

To add a port condition to an Identity Rule:

Step 1 On the identity rule editor page, select the **Ports** tab.

Step 2 Find the TCP ports you want to add from the **Available Ports**, as follows:

- To add a TCP port object on the fly, which you can then add to the condition, click the add icon ( ) above the Available Ports list.
- To search for TCP-based port objects and groups to add, click the **Search by name or value** prompt above the **Available Ports** list, then type either the name of the object, or the value of a port in the object. The list updates as you type to display matching objects. For example, if you type 443, the ASA FirePOWER module displays the provided HTTPS port object.

Step 3 To select a TCP-based port object, click it. To select all TCP-based port objects, right-click and then select **Select All**. If the object includes non-TCP-based ports, you cannot add it to your port condition.

Step 4 Click **Add to Source** or **Add to Destination**.

Step 5 Enter a **Port** under the **Selected Source Ports** or **Selected Destination Ports** list to manually specify source or destination ports. You can specify a single port with a value from 0 to 65535.

Step 6 Click **Add**.

Note The ASA FirePOWER module will not add a port to a rule condition that results in an invalid configuration.

Step 7 Click **Add** or continue editing the rule.

Adding a Zone Condition to an Identity Rule

License: Control

If the device you want to use for captive portal contains both inline and routed interfaces, you must configure a zone condition in your captive portal identity rules to target only the routed interfaces on the captive portal device.

For more information about security zones, see Working with Security Zones, page 2-32.

To add a Zone Condition to an Identity Rule:

Step 1 On the identity rule editor page, select the **Zones** tab.

Step 2 Find the zones you want to add from the **Available Zones**. To search for zones to add, click the **Search by name** prompt above the **Available Zones** list, then type a zone name. The list updates as you type to display matching zones.

Step 3 Click to select a zone. To select all zones, right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination**.

Step 5 Click **Add** or continue editing the rule.

Associating a Realm and Configuring Active Authentication Settings in an Identity Rule

License: Control

Associate the identity rule with a realm and, optionally, configure additional settings for active authentication.

To associate Identity Rules With a Realm:

Step 1 On the identity rule editor page, select the **Realm & Settings** tab.

Step 2 Select a **Realm** from the drop-down list.

Step 3 Optionally, select the **Use active authentication if passive authentication cannot identify user** check box. Note that this check box appears only when configuring a Passive Authentication rule.

Step 4 If you selected the check box in step 3, or if this is an Active Authentication rule, continue with step 4. Otherwise, skip to step 8.

Step 5 Optionally, select the **Identify as Special Identities/Guest if authentication cannot identify user** check box.

Step 6 Select an **Authentication Type** from the drop-down list.

Step 7 Optionally, **Exclude HTTP User-Agents** to exempt specific application traffic from active authentication as described in Excluding Applications From Active Authentication, page 32-11.

Step 8 Click **Add** or continue editing the rule.

Managing Realms

License: Control

To manage a Realm:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Realms**.

Step 2 If you want to delete a realm, click the delete icon ( ).

Step 3 If you want to edit a realm, click the edit icon ( ) next to the realm and make changes as described in Creating a Realm, page 32-4.

Step 4 If you want to enable or disable a realm, click the State slider next to the realm you want to enable or disable as described in Enabling or Disabling a Realm, page 32-18.

Step 5 If you want to download users and user groups on demand, click the download icon ( ) as described in Downloading Users and User Groups On-Demand, page 32-18.

Step 6 If you want to copy a realm, click the copy icon ( ).

Step 7 If you want to compare realms, see Comparing Realms, page 32-17.

Comparing Realms

License: Control

To Compare Realms:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Realms**.

Step 2 Click **Compare Realms**.

Step 3 Select **Compare Realm** from the **Compare Against** drop-down list.

Step 4 Select the realms you want to compare from the **Realm A** and **Realm B** drop-down lists.

Step 5 Click **OK**.

Step 6 If you want to navigate individually through changes, click **Previous** or **Next** above the title bar.

Step 7 Optionally, click **Comparison Report** to generate the realm comparison report.

Step 8 Optionally, click **New Comparison** to generate a new realm comparison view.

Downloading Users and User Groups On-Demand

License: Control

If you change the user or group download parameters in a realm, or if you change the users or groups on your server and want the changes to be immediately available for user control, you can force the ASA FirePOWER module to perform an on-demand user download from the server.

The maximum number of users the ASA FirePOWER module can retrieve from the server depends on your device model. If the download parameters in your realm are too broad, the ASA FirePOWER module obtains information on as many users as it can and reports the number of users it failed to retrieve in the task queue.

Before You Begin

- Enable the realm as described in Enabling or Disabling a Realm, page 32-18

To download users and user groups on-demand:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Realms**.

Step 2 Click the download icon ( ) next to the realm where you want to download users and user groups.

What to Do Next

- Optionally, monitor the task status; see the Task Status page (**Monitoring > ASA FirePOWER Monitoring > Task Status**).

Enabling or Disabling a Realm

License: Control

Only enabled realms allow the ASA FirePOWER module to query servers. To stop queries, disable the realm.

To enable or disable a realm:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Realms**.

Step 2 Click the **State** slider next to the realm you want to enable or disable.

What to Do Next

- Optionally, monitor the task status; see the Task Status page (**Monitoring > ASA FirePOWER Monitoring > Task Status**).

Managing the Identity Policy

License: Control

To manage the Identity Policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**.

Step 2 If you want to copy a policy, click the copy icon ( ).

Step 3 If you want to generate a report for the policy, click the report icon ( ).

Managing Identity Rules

License: Control

To manage Identity Rules:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**.

Step 2 If you want to edit an identity rule, click the edit icon ( ) and make changes as described in Creating an Identity Rule, page 32-12.

Step 3 If you want to delete an identity rule, click the delete icon ( ).

Step 4 Click **Store ASA FirePOWER Changes**.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-11.

Adding an Identity Rule Category

License: Control

To add an Identity Rule Category:

Step 1 On the identity rule editor page, you have the following choices:

- Select **above Category** from the first **Insert** drop-down list, then select the category above which you want to position the rule from the second drop-down list.
- Select **below rule** from the drop-down list, then enter an existing rule number. This option is valid only when at least one rule exists in the policy.
- Select **above rule** from the drop-down list, then, enter an existing rule number. This option is valid only when at least one rule exists in the policy.

Step 2 Click **OK**.

Note Rules in a category you delete are added to the category above.

Step 3 Click **Add** or continue editing the rule.