Managing Authentication and Identity Services

You can create access policies based on user identity rather than IP addresses. To enable identity-based services, you configure policies and options to obtain user identity, and then use identity objects in your access policies. The following topics describe authentication and identity services and how to configure them.

- Overview of Authentication and Identity Services, page 1
- Configuring Authentication and Identity Services, page 3

Overview of Authentication and Identity Services

Authentication is the act of confirming the identity of a user. You can obtain user identities passively or actively.

With passive authentication, user identity is obtained by checking a mapping of IP addresses to user identity collected by the CDA or AD agent application. Authentication is passive because the user is not prompted to provide credentials.

With active authentication, when an HTTP or decrypted HTTPS traffic flow comes from an IP address for which ASA CX has no user-identity mapping, you can decide whether to authenticate the user who initiated the traffic flow against the directories configured for the network. If the user successfully authenticates, the IP address is considered to have the identity of the authenticated user.

You can apply identity-based access policies to traffic that has either a passive or active user mapping, controlling network access based on who is trying to access the resource rather than controlling it by static IP address-based policies.

There are many separate features involved in providing authentication and identity services:

- Directory realms—You must define the directory realms that provide authentication services. A realm contains one or more directory servers, such as Active Directory or OpenLDAP, that define the user names and user group membership for the network. When you configure identity policies, you must select the directory realm that will provide authentication.

- Identity policies—Use identity policies to enable policies based on user identity, including username and user group membership. Identity policies never result in dropped or blocked traffic, even if the user fails to authenticate. Instead, they collect user information, so that access policies can match traffic based on user identity, and so that dashboards and events include user identity information.
• Authentication settings—Authentication settings control how authentication mappings and prompts are managed. For example, you can define how long a username-to-IP address mapping remains valid before you want to prompt the user to reauthenticate. These settings have system defaults, so you need to adjust them only if you desire different settings.

• Identity policy objects—Identity policy objects define the specific user names or user group names for which you want to define access control. You can also selectively exclude names from an object. For example, you could define an object that includes the user group Eng, but exclude users Guest1 and Guest2, who are members of that group.

• Access policies—When you specify Identity policy objects as part of the source field in an access policy, you are controlling access to the destination resources based on user identity.

• CDA or Active Directory agent—(Optional.) You can install the CDA or AD agent in your network to collect user identity information when users log into the network, before they try to pass traffic through the device. This type of identity is considered a passive identity mapping. By collecting this information, you can enable identity-based access control without forcing users to authenticate directly.

• Identity-based dashboards—Many dashboards include identity information if it is available, so you can analyze the traffic on your network based on user identity. The Users dashboard is specifically designed to provide user-based network usage information. You can use these dashboards to identify cases where network acceptable use criteria are not being met.

**Supported AAA Servers and Authentication Methods**

You can use AAA servers running LDAP (Lightweight Directory Access Protocol) to implement authentication and identity services. Following are the supported servers and the authentication methods you can use with each.

• **Microsoft Active Directory**—You can use the following AD servers. Ensure that you disable LDAP signing on the Active Directory server.
  
  • Windows Server 2008 R2
  
  • Windows Server 2003 R2

You can use the following authentication methods in identity policies when using AD; you can also allow negotiation to select the strongest supported method:

• NTLM (All Windows platforms.)

• Kerberos (Windows XP only.)

• Basic and Form (No restrictions.)

• **OpenLDAP**—Version 2.4.21 or later. The Basic and Form authentication methods are available.

**Types of User Identity**

To enable identity services, so that traffic flows can be conditionally handled based on the user who initiates the flow, the CX device maps the user name to the IP address of the user’s device.
Based on how the user-to-IP address mapping is obtained, users are considered to have one of the following identity types:

- **Active**—The user was directly authenticated by the CX device. Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.

- **Passive**—A user-to-IP address mapping was received from the Context Directory Agent (CDA) or Active Directory (AD) agent. This type of identity can be available regardless of the types of traffic sent by the user.

- **Unknown**—There is no user-to-IP mapping. For example, the user tried to actively authenticate to the CX device, but authentication failed. Users who fail active authentication are represented in user dashboards under the username `Realm\ANONYMOUS`, unless you enabled guest access, in which case the username is Guest. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address.

- **Guest**—The user failed active authentication and you enabled guest access on the identity policy. The username for these users is Guest in dashboards and events.

## What to Tell Users About Authentication

If you configure identity policies to require or allow for active authentication, users might be prompted to authenticate when they make HTTP requests, or HTTPS requests that are decrypted by decryption policies. To help users authenticate correctly, ensure that they know the following:

- Authentication prompts will include the name of the directory realm and the ASA CX management IP address. Ensure that users understand that authentication requests that include this information are valid requests and that they should respond to them.

- When using NTLM or Kerberos authentication with Active Directory, users can enter their name in any of these formats: `username`, `username@domain`, `DOMAIN\username`. For example, `user1`, `user1@example.com`, `ENG\user1`.

- When using basic authentication, users should supply their name in `username@domain` format, for example, `user1@example.com`.

## Configuring Authentication and Identity Services

The following procedure provides an overview of the process for configuring authentication and identity services. Use this procedure to understand the general configuration process and see the referenced topics for detailed steps.

### Procedure

**Step 1**  
Configure directory realms as described in Configuring Directory Realms, on page 6. The directory realms define the directory servers that contain user and user group information. Users authenticate against these servers to provide user identity, which can then be used to provide identity-based access control and reporting.
**Step 2** (Optional.) Configure the Active Directory (AD) agent as described in Identifying the Active Directory Agent, on page 22.

If you are using Active Directory in your directory realm, you can install the Context Directory Agent (CDA) or Active Directory agent to provide passive user-to-IP address mappings based on Windows login authentications.

**Step 3** (Optional.) Change the authentication settings if necessary as described in Configuring Authentication Settings, on page 23.

Authentication settings have default values appropriate for most networks, so you might not need to change them.

**Step 4** Create at least one identity policy for each directory realm as described in Configuring Identity Policies, on page 11.

Identity policies determine the type of identity users must supply, either through active authentication, passive mapping, or none at all if you elect to not require authentication. You must have at least one policy per realm, or you will not get user identity mappings for users defined within the realm.

**Note** If you intend to use active authentication, you must also ensure that the policy redirecting traffic from the ASA to the ASA CX SSP enables the authentication proxy. If you do not enable the authentication proxy, you are limited to passive authentication. For more information, see Enabling Active Authentication, on page 17.

**Step 5** If you are using active authentication, and you want to enforce authentication for HTTPS requests, configure decryption policies to decrypt secure traffic from the sources you want to authenticate. The decryption policy should apply the Decrypt Everything action.

**Step 6** (Optional.) When using Active Directory, you can configure client browsers to provide transparent authentication for NTLM or Kerberos as described in Enabling Transparent User Authentication, on page 18.

When configured to provide transparent authentication, browsers can respond to authentication requests from trusted sources by providing Windows login information without prompting users. Thus, active authentication occurs but users are not aware that authentication happened and they are not inconvenienced or confused by an unexpected authentication prompt.

**Step 7** (Optional.) Create identity-based access policies as described in Configuring Context-Aware Access Policies. You can control access to a destination by using identity policy objects in the source definition of an access policy. The identity object defines the user or user group names that are allowed, or denied, access to a destination. For information on identity policy objects, see CX Identity Objects.

**Step 8** Analyze network traffic using identity information in dashboards and events.

Many dashboards, such as the Users dashboard, includes identity-based traffic analysis. You can also access dashboards related to identity-based access policies by looking at the policy hits dashboard for the policy. Use this information to determine the efficacy of your policy and to identify users who are violating acceptable use policies. For information on dashboards, see Viewing Dashboards and Reports.

In addition to dashboards, the Event Viewer includes user name information on events when available. For information on Event Viewer, see Viewing Events.
Overview of Directory Realms

A directory realm is a named list of directory servers. For Active Directory (AD), a realm is equivalent to an AD domain. For LDAP, the realm is any LDAP server and its redundant servers, that is, all servers with the same top level distinguished name (DN).

You use directory realms:

- In identity policies, to identify the directories with which the user must authenticate. There must be an identity policy for each realm in order to use identities defined in the realm in access policies.
- On the Users page, to identify the directory that contains remote users you are granting access to the web interface.

To open the directory realms page, where you can add, edit, or delete realms and the directory servers contained in them, or reorder the directory servers within a realm, select **Components > Directory Realm**.

The Directory Realm page includes the following items:

**I want to**

Contains the following commands:

- **Add Realm**—To add a new directory realm. You are prompted for a name, description, and directory type. The realm name will appear in dashboards along with the username in the format Realm\username. Thus, you might want to use NetBIOS domain names for your realm names so that username strings include the expected NetBIOS domain name.

**List of directory realms and their directory servers**

The list shows all directory realms and within each realm is an ordered list of directory servers contained in the realm. The first server in the list is always used unless it becomes unavailable, in which case the next server in the list is tried until a response is received.

If there is more than one AD realm, you can define identity policies that use NTLM, Kerberos, or Advanced active authentication with just one of the realms. The device will bind to that AD realm, which is considered the primary realm. You can use basic and form active authentication, or passive authentication, with all realms.

To see the commands related to a directory realm or server, mouse over the directory realm header or the directory server row. The following are the available commands:

**Directory realm commands:**

- **Add New Directory**—To add a new directory server to the realm. The server is added to the top of the realm as the first entry. After adding the directory, move it to the desired position before committing your changes.
- **Delete Realm**—To delete the realm. You cannot delete a realm if it is being used in a policy or policy object, or as the global realm for system users.
- **Edit Realm**—To edit the realm properties.
Directory server commands:

- **Delete Directory**—To delete the directory server.
- **Edit Directory**—To edit the directory server properties.
- **Move Up, Move Down**—To move the directory server until it is in the desired position. The up and down commands move the directory a single row. You can also click and drag a directory to the desired location.

### Configuring Directory Realms

**Tip** Obtain the values for these settings from your AD or OpenLDAP administrator.

A directory realm is a named list of directory servers. For Active Directory (AD), a realm is equivalent to an AD domain. For LDAP, the realm is any LDAP server and its redundant servers, that is, all servers with the same top level distinguished name (DN).

To configure a directory realm, you must create the realm and then add directory servers to the realm. The following procedure explains both aspects.

**Procedure**

#### Step 1
Select **Components > Directory Realm**.

The directory realms are organized in a list, and each directory realm contains a priority list of directory servers. The first directory is always used unless it becomes unavailable, in which case subsequent directories are used. To see the commands related to a realm, you must mouse-over the name of the realm; to see commands related to a directory server, you must mouse-over the row for the directory. You can then select the desired command.

If you need to work with an existing directory realm or server, use the filter controls to help you locate the item.

#### Step 2
Configure the directory realm.

a) To open the form for creating or editing a directory realm, do one of the following:

   - To create a new realm, select **I want to > Add Realm**.
   - To edit an existing realm, mouse over the realm name and click **Edit Realm**.

b) Fill in the directory realm properties:
• **Name**—The name of the realm. This name will appear in dashboards along with the username in the format Realm\username. Thus, you might want to use NetBIOS domain names for your realm names so that username strings include the expected NetBIOS domain name. The name is also visible to end users if you create an identity policy for the realm that results in users occasionally being prompted to authenticate.

• **Description**—A description for the realm.

• **Directory Type**—The type of directory server, either Microsoft Active Directory or Standard LDAP.

Select SSO if you are creating a single-sign-on (SSO) directory for integration with other management products. For detailed information on creating an SSO realm, see Configuring SSO Directories and Users.

• **Primary Domain**—(AD only.) The fully qualified Active Directory domain name that the device should join. For example, example.com. Create separate realms for each domain, even if there are trust relationships among the domains.

• **Join Username, Join Password**—(AD only.) The Active Directory sAMAccountName or User Principal Name to use when joining the device to the AD domain or to leave the domain. These credentials must have the authority within AD to join devices to the domain or to leave the domain.

c) (AD only.) Click the Test Domain Join link to verify that you can join the device to the AD realm. If the test fails, you need to resolve the issues. Log into the CLI and use the show dns command to verify that you have configured the right DNS domain for the device, and included the domain in the search domains list. Another potential problem might be that intervening firewalls do not have all required ports open to enable domain join; see the Microsoft support site for details on how to configure a firewall for domains and trusts for specific port requirements for your setup.

d) Click Save to save your changes.

**Step 3**  
Configure the directory servers within a realm:

a) To open the form for adding or editing a directory server, do one of the following:

   • To add a directory server, mouse over the realm name and click Add New Directory.
   
   • To edit an existing directory server, mouse over the server name and click Edit Directory.

b) Fill in the directory server properties. For detailed information, see Directory Properties, on page 8.  

   **Tip**  Be sure to click the Test Connection link when filling in the properties. This will test whether the directory can be contacted using those properties. If the connection fails and you are certain the properties are correct, ensure there is a network path between the device and the directory server. If necessary, log into the CLI to use commands such as ping and traceroute.

c) Click Save to save your changes.  
You can repeat the process of adding directories to identify all servers used in the realm.

**Step 4**  
If necessary, move the server entries so that they are in priority order within the directory realm, with the primary server at the top of the list. You can drag and drop server entries, or use the Move Up or Move Down links that appear when you mouse over a server entry.
Directory Properties

Tip
Obtain the values for these settings from your AD or OpenLDAP administrator.

The following table describes properties for directories that you include in directory realms. Where indicated, some properties apply to certain directory types only. For more information about LDAP properties and their syntax, refer to RFC 2253.

Table 1: Directory Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Hostname</td>
<td>The DNS name or IP address of the directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used for communications with the server. The default is 389. Note: Port 389 is the only supported port, which supplies standard LDAP (plain text) connections. You cannot use secure LDAP (LDAP over SSL) on port 636, nor can you specify the Active Directory Global Catalog Server on port 3268.</td>
</tr>
<tr>
<td>LDAP Login Name</td>
<td>The distinguished name of the directory object in the LDAP hierarchy used for authenticated binding. The LDAP login name represents a user record in the LDAP server that the administrator uses for binding (administrator privileges are not required for the user). For example, cn=Administrator,dc=example,dc=com. This string is case-sensitive and alphanumeric. Special characters are allowed. (LDAP only.)</td>
</tr>
<tr>
<td>AD Login Name</td>
<td>The user name used for authenticated binding with the AD server, for example, <a href="mailto:username@example.com">username@example.com</a>. For Active Directory, the user privilege requirements differ based on the type of authentication you will allow in your identity policies. Ensure you specify a user with the required privileges:</td>
</tr>
<tr>
<td></td>
<td>• NTLM, Basic—Any valid user account should work.</td>
</tr>
<tr>
<td></td>
<td>• Kerberos—The user account must have the &quot;Validated Write to Service Principle Name&quot; permission. See the Active Directory documentation for details on delegating authority to modify SPNs.</td>
</tr>
<tr>
<td>AD/LDAP Password</td>
<td>The password for the user specified in AD/LDAP Login Name.</td>
</tr>
</tbody>
</table>
### Property | Description
--- | ---
**User Search Base** | The LDAP search base distinguished name used to fully-qualify usernames being authenticated against LDAP directories. The field also defines the location in the LDAP hierarchy for searching or querying user information in both LDAP and AD. For example, `cn=users,dc=example,dc=com`. The maximum length is 128 characters. The string is case-sensitive. Spaces are not permitted, but other special characters are allowed.

If you do not specify a user search base, the system will create a generic one consisting of the entire domain components of the directory name. For example, if the directory name is `ad.example.com`, the constructed qualifier would be `dc=example,dc=com`. The generic name might or might not work in your network, so it is best to explicitly enter a qualifier. For standard LDAP, you probably will always need to explicitly enter a qualifier. If you use an IP address instead of a DNS name, you will always need to enter a qualifier.

For more information, see [Determining the Directory Search Base](#), on page 10.

**Group Search Base** | The LDAP search base distinguished name used to search individual groups for user membership for authorization against LDAP directories. The field also defines the location in the LDAP hierarchy for searching or querying user group information in both LDAP and AD. For example, `ou=groups,dc=example,dc=com`. The maximum length is 128 characters. The string is case-sensitive. Spaces are not permitted, but other special characters are allowed.

If you do not specify a group search base, the system will create a generic one consisting of the entire domain components of the directory name. For example, if the directory name is `ad.example.com`, the constructed qualifier would be `dc=example,dc=com`. The generic name might or might not work in your network, so it is best to explicitly enter a qualifier. If you use an IP address instead of a DNS name, you will always need to enter a qualifier.

For more information, see [Determining the Directory Search Base](#), on page 10.

**Note** It is possible, but not necessary, that the user and group search base is the same string.

**Group Attribute** | The LDAP attribute that lists all users that belong to a group. Select one of the following:

- **member**—The normal group attribute for Active Directory.
- **uniqueMember**—The normal group attribute for OpenLDAP.
- **Custom**—Select this option if you created a custom group attribute in your directory, such as `UserInGroup`, and enter the attribute value in the field provided.

**Test Connection link** | Tests whether the properties you entered will successfully connect to the directory server. If the connection fails, check your settings. If you are certain they are correct, check whether there is a network path between the device and the directory.
Determining the Directory Search Base

When you configure directory properties, you need to specify the user and group search bases. These bases are defined in your directory server, and differ from network to network. You must enter the correct bases for identity policies to work. If the bases are wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.

Tip
To get the correct bases, consult the administrator who is responsible for the directory servers.

For active directory, you can determine the correct bases by logging into the Active Directory server as domain administrator, and using the dsquery command at a command prompt as follows to determine the bases:

User search base
Enter the dsquery user command with a known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John" to return information for all users that start with "John."

C:\Users\Administrator>dsquery user -name "John"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

The user search base would be "DC=csc-lab,DC=example,DC=com."

Group search base
Enter the dsquery group command with a known group name to determine the base distinguished name. For example, the following command uses the group name Employees to return the distinguished name:

C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

The group search base would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the Active Directory structure (Start > Run > adsiedit.msc). In ADSI Edit, right click any object, such as an organizational unit (OU), group, or user, and choose Properties to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:
1 Click the Test Connection button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.
2 Commit changes to the device.
3 Select Components > Objects and then I want to > Add CX Identity Object. Try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully. If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base.
Deleting Directory Realms or Directories

You can delete directories within a realm, or you can delete the entire directory realm. However, you cannot delete a directory realm if it is currently being used in a policy or policy object, or as the global realm for system users.

Procedure

Step 1 Select Components > Directory Realm.
Step 2 Do any of the following:
  • To delete a directory server from a directory realm, mouse over the server name within the realm and click Delete Directory.
  • To delete a directory realm, mouse over the name of the realm and click Delete Realm.

Configuring Identity Policies

Use identity policies to enable policies based on user identity, including username and user group membership. Identity policies never result in dropped or blocked traffic, even if the user fails to authenticate.

Instead, identity policies can prompt users to provide username/password when attempting to connect to a destination according to your matching criteria and authentication action. If the user fails authentication, the user’s traffic is evaluated against your access rules and is permitted or denied based on those rules. If no passive authentication mapping is available for the IP address of the workstation the user is using, only the user’s IP address is used for matching purposes, so any identity-based rules you create will not apply.

Thus, you might have an identity-based access rule that would allow traffic for UserA to ServerA, and disallows all other access to ServerA. If UserA successfully authenticates, the access rule will apply and UserA will be allowed to access ServerA. If UserA fails authentication, and there is no passive mapping, the access rule will not apply and UserA will not be allowed access to ServerA.

Tips

  • By active or passive authentication, you can ensure that the user associated with a traffic flow is known, allowing identity-based access rules to function correctly, and providing user information in dashboards and events.

  • Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted. Thus, it is not necessary to create Do Not Require Authentication policies for non-HTTP/HTTPS traffic. Likewise, it is not meaningful to create a policy that applies the Get Identity via Active Authentication action for traffic matching criteria that excludes HTTP traffic, for example, by selecting a service group that specifies ICMP as the only service type.

  • Identity policies are applied based on first match for traffic matching criteria. Ensure that you define the matching criteria precisely so that the desired action, including the directory realm to use, is applied to each traffic class.
Before You Begin

You must create the directory realm before you can configure identity policies for the realm. (Single Device mode only.) When you create the first directory realm, a default identity policy is automatically created for the realm. You can edit or delete the default policy to suit your needs.

Procedure

Step 1  Select Configurations > Policies/Settings and open the Identity Policies tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2  Do any of the following:

• To add a new policy, use one of the Add Policy buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.

• To edit an existing policy, select the policy and click the Edit Policy button.

• To base a new policy on a similar existing policy, select the policy and click the Duplicate Policy button.

A form opens with the policy properties.

Step 3  Define the traffic matching criteria using the Source, Destination, and Service fields. You can leave any field blank to not restrict traffic based on that criteria.

Step 4  Select the directory realm in the Realm field.

Step 5  Define the action to apply to matching traffic, including authentication type and user agents if necessary. For detailed information about the action-related settings, read Identity Policy Properties, on page 13. Consider the following tips:

• The available options differ based on directory type and whether you configured a CDA or AD agent.

• If you select an option that allows for active authentication, either Get Identity via Active Authentication or Get Identity Using AD Agent with Yes selected for the active authentication question, you can exclude user agents from active authentication. Exclude agents that cannot respond to active authentication prompts, for example, software update applications.

• With active authentication, you also select the authentication method: basic or form (for all realm types), plus NTLM, Kerberos, or Advanced (AD only). Select the method supported by your server and clients; select Advanced if you support Kerberos, NTLM, and basic. If you have more than one AD realm, you can use NTLM, Kerberos, or Advanced with a single AD realm only; all other AD realms must use basic or form.

  Note  If you select form, you can customize the active authentication login form presented to the user on the End User Notification page (select Administration > End User Notification).

Step 6  If you want to limit the policy to traffic on specific interfaces on the parent device, select the Source Interface Role or the Destination Interface Role, or both, that identify the interfaces.

The default is to apply the policy to traffic between any interfaces on the device. If you select interfaces that do not exist on the device, the policy is never applied to traffic.

Step 7  Click Save Policy.

Step 8  If necessary, move the policy so that it is in priority order.
Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

### Identity Policy Properties

Use identity policies on CX devices to define the user authentication requirements for matching traffic. Identity policies never result in blocked traffic. Instead, they determine whether user identity is obtained for the source IP address of a traffic flow.

Requiring authentication makes it possible to configure access policies based on user identity, and provides user-based usage information in dashboards.

Identity policies have the following properties:

**Policy Name**

The name of the policy. This name appears in Event Viewer for authentication events generated by traffic that matches this policy, so choose a name that will help you analyze event data.

**Enable Policy: On/Off**

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.
Traffic Matching Criteria

The traffic matching criteria that identifies the traffic to which the policy applies. To match the policy, the flow must match every specified property, that is, there is an AND relationship between the properties. Use the default Any selection if you do not want to restrict the policy based on that condition. Leave all fields with the default Any to match every possible traffic flow.

All of the following criteria are used to determine the traffic to which a policy applies.

- **Source**—A list of network groups. If a packet matches any selected object, it is considered to satisfy the source condition.

- **Destination**—A list of network groups. If a packet matches any selected object, it is considered to satisfy the source condition.

- **Service**—A list of service groups that define protocol and port combinations. If a packet matches any selected object, it is considered to satisfy the service condition.

**Note**

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device for source or destination criteria, or ASA service objects for the service criteria. The network group objects come in two types: one that can be used on both ASA and CX devices, and one that can be used on CX devices only, which is explicitly called CX network group.

For information on how to select items, including how to add, edit, or remove them, filter the selection list, create or edit objects, or view object contents, see Selecting Items.

**Realm**

The directory realm used to authenticate traffic. If the user is prompted for authentication, servers in this realm are used to verify the credentials supplied by the user.
Managing Authentication and Identity Services

Configuring Identity Policies

Action
The type of authentication required for matching traffic flows. The options differ based on the directory type and whether you configured a CDA or AD agent. Select one of these options based on availability:

Get Identity Using AD Agent
(AD with configured CDA or AD agent only.) If a passive user-to-IP address mapping was obtained from the CDA or AD agent, use it.
Select Yes or No for Do you want to use active authentication if AD agent cannot identify the user? If you select Yes (the default), and a passive mapping for the user’s IP address was not obtained from the CDA or AD agent, the system tries to get identity through the client, either transparently (NTLM, Kerberos only) or by prompting the user to authenticate.
If you select No, and a passive mapping is not available, the user’s IP address will not be associated with a user name, and identity-based access rules will not be applied to the user’s traffic.

Get Identity via Active Authentication
(All directory types.) Obtain identity information even if a passive mapping exists for the user. Identity is obtained transparently if you use NTLM or Kerberos and the clients have the correct configuration; otherwise, users are prompted to authenticate.
Once authenticated, the user’s IP address is considered a surrogate for the user, and the user is not required to reauthenticate for every subsequent connection. Reauthentication is required after the authenticated session duration setting is exceeded.

Do Not Require Authentication
(All directory types except AD with a configured CDA or AD agent.) Do not obtain user identity. Identity-based access rules will not be applied to the user’s traffic.

Note
Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.

Do you want to use guest access if active authentication cannot identify user?: Yes/No
If you select an option that requires or allows for active authentication, select whether users who fail active authentication are labeled as Guest users. These users will match the Guest Users identity object. You can write access policies to provide special handling for this category of user. These users appear in dashboards and events under the Guest username.
If you select No, users who fail active authentication map to the Unknown Users identity object. You can also write access policies for unknown users.
Authentication Type

If you select an option that requires or allows for active authentication, select the authentication method to use during active authentication. You can use the following authentication methods; select one for which your directory servers are configured:

- **NTLM** (NT LAN Manager, AD realms only). Supported by all Windows platforms.
- **Kerberos** (AD realms only). Supported for Windows XP only.
- **Basic**. This is the default. Supported on all platforms.
- **Advanced** (AD realms only). Select this option to allow the device to negotiate the method between the user agent (the application the user is using to initiate the traffic flow) and the Active Directory server. Negotiation results in the strongest commonly supported method being used, in order, Kerberos, NTLM, then basic.
- **Form**. This is a type of basic authentication, where the user is presented with a login browser page. You can customize the active authentication form on the End User Notification page (select Administration > End User Notification). Supported on all platforms.

If you allow for NTLM or Kerberos, clients can configure their browsers to allow for transparent authentication as described in Enabling Transparent User Authentication, on page 18. Otherwise, users are prompted for their directory username and password.

---

**Note**

If you have more than one AD realm, you can use NTLM, Kerberos, or Advanced with a single AD realm only; all other AD realms must use basic or form.

---

Exclude User Agent

If you select an option that requires or allows for active authentication, you can exclude user agents (applications) that cannot respond to authentication requests, such as software update applications or remote access VPN clients that send authentication traffic through the VPN tunnel (such as Android 2.3 with AnyConnect 2.5). Select the user agent policy objects that identity the user agents (in the Include list in the object) that you do not want to prompt for authentication.

Interface Roles

The criteria that identifies the parent device’s interfaces to which the policy applies. To match the policy, the traffic must enter the device on one of the source interfaces and leave the device on one of the destination interfaces. The default is any interface for both source and destination, meaning the policy is not restricted to specific interfaces.

To limit the policy to specific interfaces, select the appropriate interface role objects in either the Source Interface Role or Destination Interface Role fields, or both. The interface role objects define the interface names or naming patterns for the interfaces.

---

**Tip**

If you specify interface roles, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.
Enabling Active Authentication

If you want to use active authentication, you need to address the following requirements:

- The class map for the traffic redirection policy on the ASA must include the auth-proxy keyword, for example `cxsc fail-open auth-proxy`.
  
  If you configure redirection using PRSM, the keyword is automatically included.

- The default port used by the ASA for active authentication is tcp/885. You can configure a different port using the `cxsc auth-proxy port number` command using the ASA CLI. A non-default port must be higher than 1024. You can see the currently configured port using the `show run all cxsc` command.

- If there are firewalls between the ASA and the user, you must open the authentication port on those firewalls.

- Ensure that time settings are consistent among the directory servers, ASA CX, and clients. A time shift among these devices can prevent successful user authentication. "Consistent" means that you can use different time zones, but the time should be the same relative to those zones; for example, 10 AM PST = 1 PM EST.

- When using Active Directory with Kerberos authentication, the domain controller, ASA CX, and client must all be in the same domain, or authentication will fail. For NTLM and basic authentication, the devices should be in the domain, but authentication might work even if they are not in the same domain. Although NTLM is supported with all Windows clients, Kerberos is supported with Windows XP clients only.

  To increase the likelihood of successful authentication, consider selecting Advanced as the authentication method. This will allow the system to negotiate the strongest method supported by both the client and server, and to try different methods if one fails.

- If you use Kerberos or NTLM with Active Directory, you can configure browsers to transparently respond to active authentication requests. For detailed information, see Enabling Transparent User Authentication, on page 18.

- Not all user agents can successfully respond to active authentication requests. For example, if a user agent in a remote access VPN connection sends the authentication traffic through the VPN tunnel, active authentication will not succeed. Android 2.3 using AnyConnect 2.5 is an example of this type of agent. Software updaters might also not successfully respond to active authentication.
To account for these types of user agent, you can use an existing user agent object, or you can create a user agent policy object that lists these agents in the Include list. Then, in the active authentication identity policy, select the objects in the Exclude User Agent field.

- Users are prompted only if the traffic is HTTP or decrypted HTTPS. To prompt for HTTPS flows, you must create decryption policies that apply the Decrypt Everything action to the appropriate traffic sources.

**Special Configuration Requirements for Remote Access VPN**

If the ASA hosts remote access AnyConnect VPN connections, the active authentication prompt might not be displayed for certain clients. For example, Windows 7 Enterprise and Professional Editions, and Mac OS X 10.6.8, clients have this problem.

To enable active authentication prompting in these cases, you need to configure a split tunnel policy on the VPN access group to exclude the ASA’s Internet IP address from the VPN. The following example shows what such a configuration would look like.

```
ASA-5525-3# show running-config interface
interface GigabitEthernet0/4
   nameif internet
   security-level 100
   ip address 10.194.204.37 255.255.255.0
ASA-5525-3# show running-config access-list
access-list Split_Tunnel_List standard permit host 10.194.204.37
ASA-5525-3# show running-config group-policy
group-policy test internal
group-policy test attributes
   vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
   split-tunnel-policy excludespecified
   split-tunnel-network-list value Split_Tunnel_List
ASA-5525-3#
```

**Enabling Transparent User Authentication**

If you configure the identity policy for a realm to allow for active authentication, either Get Identity via Active Authentication or Get Identity Using AD Agent with Yes selected for the active authentication question, you can use the following authentication methods to acquire user identity:

**Basic Authentication (Active Directory and LDAP)**

With basic authentication, users are always prompted to authenticate with their directory username and password. The password is transmitted in clear text. For that reason, basic authentication is not considered a secure form of authentication.

Basic is the default authentication mechanism.

**Form (Active Directory and LDAP)**

This is a type of basic authentication, where the user is presented with a login browser page. You can customize the active authentication form on the End User Notification page (select Administration > End User Notification). Users are always presented with the login form.
**Integrated Windows Authentication (Active Directory only)**

With integrated Windows authentication, you take advantage of the fact that users log into a domain to use their workstation. The browser tries to use this domain login when accessing a server, or in the case of ASA CX, the network protected by the ASA CX. The password is not transmitted. If authentication is successful, the user is transparently authenticated; the user is unaware that any authentication challenge was made or satisfied.

If the browser cannot satisfy an authentication request using the domain login credentials, the user is prompted for username and password, which is the same user experience as basic authentication. Thus, if you configure integrated Windows authentication, it can reduce the need for users to supply credentials when accessing the network or servers in the same domain.

You must configure client browsers to support integrated Windows authentication to enable transparent authentication. The configuration is explained below.

When you configure an authentication policy, you select the specific type of authentication method used in your network. The options are:

- **NTLM.** Supported by all Windows platforms.
- **Kerberos.** Supported by Windows XP only.
- **Advanced,** where the strongest method allowed by both the Active Directory server and the user agent is used. (The user agent is typically a web browser through which the user is initiating a traffic flow.) The order of strength is Kerberos, NTLM, then basic.

The following sections explain the general requirements and basic configuration of integrated Windows authentication for some commonly used browsers that support it; users should consult the help for their browser (or other user agent) for more detailed information, because the techniques can change between software releases.

---

**Tip**

Not all browsers support integrated Windows authentication, such as Chrome and Safari (based on the versions available when this was written). Users will be prompted for username and password. Consult the browser’s documentation to determine if support is available in the version you use.

---

**Requirements for Transparent Authentication**

Users must configure their browser or user agent to implement transparent authentication. They can do this individually, or you can configure it for them and push the configuration to client workstations using your software distribution tools. If you decide to have users do it themselves, ensure that you provide the specific configuration parameters that work for your network.

Regardless of browser or user agent, you must implement the following general configuration:

- **Add the ASA interface through which users connect to the network to the Trusted Sites list.** You can use the IP address or if available, the fully-qualified domain name (for example, asa_inside.example.com). You can also use wildcards or partial addresses to create a generalized trusted site. For example, you can typically cover all internal sites using *.example.com or simply example.com, trusting all servers in your network. If you add the specific address of the ASA interface, you might need to add several addresses to the trusted sites to account for all user access points to the network.

- **Integrated Windows authentication does not work through a proxy server.** Therefore, you must either not use a proxy, or you must add the ASA interface to the addresses excluded from going through the
proxy. If you decide that you must use a proxy, users will be prompted for authentication even if you use the NTLM or Kerberos methods.

**Tip**
Configuring transparent authentication is not a requirement, but a convenience to end users. If you do not configure transparent authentication, users are presented with a login challenge for all authentication methods.

---

**Configuring Internet Explorer for Transparent Authentication**

To configure Internet Explorer for both NTLM and Kerberos transparent authentication:

**Procedure**

**Step 1**
Select **Tools > Internet Options**.

**Step 2**
Select the **Security** tab, select the **Local Intranet** zone, then do the following:

a) Click the **Sites** button to open the list of trusted sites.

b) Ensure that at least one of the following options is selected:

- **Automatically detect intranet network**. If you select this option, all other options are disabled.
- **Include all sites that bypass the proxy**.

c) Click **Advanced** to open the Local Intranet Sites dialog box, then paste the URL you want to trust into the **Add Site** box and click **Add**.

Repeat the process if you have more than one URL. Use wildcards to specify a partial URL, such as `http://*.example.com` or simply `*.example.com`.

Close the dialog boxes to return to the Internet Options dialog box.

d) With **Local Intranet** still selected, click **Custom Level** to open the Security Settings dialog box. Find the **User Authentication > Logon** setting and select **Automatic logon only in Intranet zone**. Click **OK**.

**Step 3**
In the Internet Options dialog box, click the **Connections** tab, then click **LAN Settings**.

If **Use a proxy server for your LAN** is selected, you need to ensure that the ASA interface bypasses the proxy. Do any of the following as appropriate:

- **Select Bypass proxy server for local addresses**.
- **Click Advanced** and enter the address into the **Do not use proxy server for addresses beginning with** box. You can use wildcards, for example, `*.example.com`.

---

**Configuring Firefox for Transparent Authentication**

Firefox has different properties for NTLM and Kerberos authentication. The following steps explain the configuration for both methods. If you do not support both methods, skip the steps for the unsupported method.
Procedure

Step 1  Open about:config. Use the filter bar to help you locate the preferences that you need to modify.

Step 2  To support NTLM, modify the following preferences (filter on network.automatic):

- `network.automatic-ntlm-auth.trusted-uris`—Double-click the preference, enter the URL, and click OK. You can enter multiple URLs by separating them with commas; including the protocol is optional. For example:

  http://host.example.com, http://hostname, myhost.example.com

  You can also use partial URLs. Firefox matches the end of the string, not a random substring. Thus, you could include your entire internal network by specifying just your domain name. For example:

  example.com

- `network.automatic-ntlm-auth.allow-proxies`—Ensure that the value is `true`, which is the default. Double-click to change the value if it is currently false.

Step 3  To support Kerberos, modify the following preferences (filter on network.negotiate):

- `network.negotiate-auth.allow-proxies`—Ensure that the value is `true`, which is the default. Double-click to change the value if it is currently false.

- `network.negotiate-auth.delegation-uris`—Double-click and enter http://,https://.

- `network.negotiate-auth.gsslib`—Ensure that the value is blank, which is the default. If this preference has a value, right-click it and select Reset, or double-click it and erase the value.

- `network.negotiate-auth.trusted-uris`—Double-click and enter http://,https://.

- `network.negotiate-auth.using-native-gsslib`—Ensure that the value is `true`, which is the default. Double-click to change the value if it is currently false.

Step 4  Check the HTTP proxy settings. You can find these by selecting Tools > Options, then click the Network tab in the Options dialog box. Click the Settings button in the Connection group.

- If **No Proxy** is selected, there is nothing to configure.

- If **Use System Proxy Settings** is selected, you need to modify the `network.proxy.no_proxies_on` property in about:config to add the trusted URIs you included in `network.automatic-ntlm-auth.trusted-uris` (or would have included, if you configured Kerberos only).

- If **Manual Proxy Configuration** is selected, update the **No Proxy For** list to include these trusted URIs.

- If one of the other options is selected, ensure that the properties used for those configurations exclude the same trusted URIs.
Identifying the Active Directory Agent

The Cisco Context Directory Agent (CDA) or Cisco Active Directory (AD) Agent provides user-to-IP address mappings to all devices that are configured to use it. For users who log into the network domain on your standard (non-VPN) network, the agent, in communication with the AD server, obtains the login information and creates a user-to-IP address mapping table. This information can be augmented by other devices in the network, such as the ASA, which can provide mappings obtained from VPN and direct sources. Identity mappings obtained from the AD agent are considered passive mappings.

Both the ASA and CX devices use the same CDA or AD agent setup to enable identity-aware firewall services. CDA replaces the older AD agent software, but the web interface uses "AD agent" to refer to either application.

Tip

Configuring a CDA or AD agent is optional. Configure it only if you want to support passive mappings. Note that if you do not support passive mappings, you must use active authentication in your identity policies or you will not have user names available for access control, and events and dashboards will not include user information.

Before You Begin

CDA and AD agent are separate software that you must install in your network. You must configure one of them to work with the Active Directory servers and with the network devices that are its consumer devices or clients. Before completing this task, install and configure the agent software.

Obtain the CDA or AD agent software from http://www.cisco.com/go/asa.

For information on setting up and configuring the software, see the following documents:


You must add the CX device as a consumer device (CDA) or client (AD agent), which you can do before or after you complete this procedure. Keep in mind that the RADIUS shared secret configured for the CX device on the CDA or AD agent and the one configured here must be the same.

Procedure

Step 1 Select Configurations > Policies/Settings and open the AD Agent tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2 Enter the following information:

- **Hostname or IP**—The DNS name or IP address of the CDA or AD agent server.
- **Password**—The RADIUS shared secret that is configured on the CDA or AD agent for use with this client device.

Step 3 Click Test to check whether the agent can be contacted using the supplied information.
If the connection fails, check your settings. If you are certain they are correct, check whether there is a network path between the device and the agent.

**Step 4**  
If available, configure the secondary agent.  
If you have a secondary agent configured for the device, click **Add Secondary CDA Agent**, fill in the address and password, and test the connection. If the primary becomes unavailable, the secondary will be used to obtain mappings. This provides a high-availability setup for the agent.

**Step 5**  
Click **Save** to save your changes.

---

**What to Do Next**

CDA or AD agent mappings are used only if you allow for passive mappings in the identity policies for the realm that contains the AD servers that are also clients of the agent. Thus, you should check your identity policies to ensure they specify **Get Identity Using AD Agent**. If your policies use **Get Identity via Active Authentication**, then the passive mappings are not used.

Ensure that you define directory realms for each AD domain for which the agent collects identity information.

---

**Configuring Authentication Settings**

You can configure authentication settings related to how your identity policies function.

**Procedure**

**Step 1**  
Select **Configurations > Policies/Settings** and open the **Auth Settings** tab.  
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Step 2**  
Change the following options as needed:

- **Authenticated session duration**—The number of hours for which a user-to-IP address mapping will be maintained. When a mapping reaches this age, it is deleted and a new mapping is obtained based on your identity policy settings. For example, if you use active authentication for the realm that matches the user’s IP address, the user will be authenticated during the user’s next connection attempt. However, if your policy uses passive mappings and does not allow for active authentication, the user will not be authenticated.

- **Failed authentication timeout**—If a user fails to correctly authenticate during active authentication, and exceeds the maximum authentication attempts, the IP address for the user is considered to have failed authentication. This timeout value determines the length of time, in minutes, before the user at that IP address is again prompted to authenticate. During this time, all traffic from the IP address is evaluated based on the IP address alone, and no user or user group based rules are applied to the traffic. Thus, during this failed timeout period, a user might be prevented from accessing resources for which the user would be allowed if the user had successfully authenticated.

- **Maximum authentication attempts**—The number of times a user can retry authentication when prompted to authenticate by ASA CX. The number of attempts is reset when the user successfully authenticates. If the user fails to authenticate, the user is not again prompted for authentication until the failed authentication timeout is exceeded.
• **Group refresh interval**—How often user group membership is updated from the directory servers, in hours. The default is every 24 hours (once a day). If you add a user to a group, the user is not recognized as being a member of the group until the next update. Membership for a group is obtained only if you use the group in a policy.

• **Guest user access timeout**—If a user fails active authentication and becomes a guest user, the length in time, in hours, that the user will remain a guest. After the timeout is passed, the user will again be prompted to authenticate. There is no limit to how often the user can be a guest.

**Step 3**  
Click **Save** to save your changes.