Controlling Traffic Based on Users

Access control rules within access control policies exert granular control over network traffic logging and handling. User conditions in access control rules allow you to perform user control—to manage which traffic can traverse your network, by limiting traffic based on the LDAP user logged into a host.

User control works by associating access-controlled users with IP addresses. Deployed agents monitor specified users as they log in and out of hosts or authenticate with Active Directory credentials for other reasons. For example, your organization may use services or applications that rely on Active Directory for centralized authentication.

For traffic to match an access control rule with a user condition, the IP address of either the source or destination host in the monitored session must be associated with a logged in access-controlled user. You can control traffic based on individual users or the groups those users belong to.

You can combine user conditions with each other and with other types of conditions to create an access control rule. These access control rules can be simple or complex, matching and inspecting traffic using multiple conditions. For detailed information on access control rules, see Tuning Traffic Flow Using Access Control Rules, page 14-1.

Note

Hardware-based fast-path rules, Security Intelligence-based traffic filtering, and some decoding and preprocessing occur before network traffic is evaluated by access control rules. You can also configure the SSL inspection feature to block or decrypt encrypted traffic before access control rules evaluate it.

User control requires a Control license and is supported only for LDAP users and groups (access-controlled users), using login and logoff records reported by a User Agent monitoring Microsoft Active Directory servers.

However, with only a FireSIGHT license you can still take advantage of user awareness, which is the basis of user control. User awareness allows you to view agent-reported user activity as well as additional activity for non-access-controlled users, which the system can detect when managed devices examine allowed network traffic for discovery data. The system can identify login attempts over various protocols: AIM, IMAP, LDAP, Oracle, POP3, SIP, FTP, HTTP, and MDNS.

To add context to the user activity reported by the system, you can query an LDAP server in your deployment to retrieve metadata for not only access-controlled users, but also some non-access-controlled users: POP3 and IMAP users detected by user discovery and LDAP users whose activity is detected by either user discovery or a User Agent.

User awareness allows all types of deployments to determine the “who” behind the “what.” For example, you could determine:

- who is attempting unauthorized access of a server that has high host criticality
- who is consuming an unreasonable amount of bandwidth
• who has not applied critical operating system updates
• who is using instant messaging software or peer-to-peer file-sharing applications in violation of company IT policy
• who owns the host targeted by an intrusion event that has a Vulnerable (level 1: red) impact level (requires Protection)
• who initiated an internal attack or portscan (requires Protection)

Armed with this information, you can take a targeted approach to mitigate risk, and take action to protect others from disruption. User control adds the ability to block LDAP users and user activity. Together, user awareness and control capabilities significantly improve audit controls and enhance regulatory compliance. For more information, see Understanding User Data Collection, page 45-3.

The following table lists the requirements for user awareness and control. For detailed, up-to-date information on User Agents, see the User Agent Configuration Guide.

Table 17-1 Requirements for User Awareness and Control

<table>
<thead>
<tr>
<th>Requirement</th>
<th>User Awareness</th>
<th>User Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>license</td>
<td>FireSIGHT Control</td>
<td>Control</td>
</tr>
<tr>
<td>devices</td>
<td>Any</td>
<td>Any except Series 2 or X-Series</td>
</tr>
<tr>
<td>Defense Centers</td>
<td>Any</td>
<td>Any except DC500</td>
</tr>
</tbody>
</table>
| User Agent                              | Install Version 2.2 of the User Agent on a Windows computer running one of the following, with TCP/IP access to and from the Defense Center and Microsoft Active Directory servers you want to monitor:
  • Windows Vista, Windows 7, or Windows 8
  • Windows Server 2008 or 2012
| LDAP server for user metadata retrieval | One of the following, with TCP/IP access from the Defense Center:
  • Microsoft Active Directory on Windows Server 2008 (required for user control)
  • Oracle Directory Server Enterprise Edition 7.0 on Windows Server 2008 (user awareness only)
  • OpenLDAP on Linux (user awareness only)

For more information, see:
• Adding a User Condition to an Access Control Rule, page 17-2
• Retrieving Access-Controlled Users and LDAP User Metadata, page 17-4
• Using User Agents to Report Active Directory Logins, page 17-9

Adding a User Condition to an Access Control Rule

License: Control

Supported Devices: Any except Series 2 or X-Series
Supported Defense Centers: Any except DC500

The FireSIGHT System’s user control feature works by associating access-controlled users with host IP addresses. Deployed User Agents monitor specified users as they authenticate with Microsoft Active Directory credentials. For traffic to match an access control rule with a user condition, the IP address of either the source or destination host in the monitored session must be associated with a logged in access-controlled user.

Before you can perform user control, you must:

- Configure a connection between the Defense Center and a Microsoft Active Directory server; see Retrieving Access-Controlled Users and LDAP User Metadata, page 17-4.

Caution

If you configure a large number of user groups to monitor, or if you have a very large number of users mapped to hosts on your network, the system may drop user mappings based on groups, due to memory limitations. As a result, access control rules based on user groups may not fire as expected.

You can add a maximum of 50 users and groups to the Selected Users in a single user condition. Conditions with user groups match traffic to or from any of the group’s members, including members of any sub-groups, with the exception of individually excluded users and members of excluded sub-groups.

Note

Before you can perform user control using a group criterion, the system must detect activity from at least one user in that group. This initial connection is not handled by the access control rule it matches, but instead by the next rule it matches, or the access control policy default action.

When building a user condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

To control user traffic:

**Access:** Admin/Access Admin/Network Admin

**Step 1**
In the access control policy that targets the devices where you want to control traffic by LDAP user or group, create a new access control rule or edit an existing rule.

For detailed instructions, see Creating and Editing Access Control Rules, page 14-2.

**Step 2**
In the rule editor, select the Users tab.

The Users tab appears.

**Step 3**
Find and select the users and groups you want to add from the Available Users list.

Users and groups are marked with different icons. To search for users and groups to add, click the Search by name or value prompt above the Available Users list, then type the name of the user or group. The list updates as you type to display matching items.

To select an item, click it. To select multiple item, use the Shift and Ctrl keys, or right-click and then select Select All.

**Step 4**
Click Add to Rule to add the selected users and groups to the Selected Users list.

You can also drag and drop selected users and groups.

**Step 5**
Save or continue editing the rule.
You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Retrieving Access-Controlled Users and LDAP User Metadata

License: FireSIGHT or Control
Supported Devices: feature dependent
Supported Defense Centers: feature dependent

Before you can perform user control (that is, write access control rules with user conditions), you must configure a connection between the Defense Center and at least one of your organization’s Microsoft Active Directory servers. The Defense Center regularly and automatically queries the LDAP server to update metadata for access-controlled users, that is, the users and groups whose activity you want to monitor with User Agents, and who you can use as criteria when limiting traffic. The Defense Center also retrieves metadata for non-access-controlled users whose activity has already been reported by a User Agent. Alternately, you can perform an on-demand query.

If you are not performing user control, you can query additional types of LDAP server for user awareness data—metadata associated with POP3 and IMAP users as well as LDAP users whose activity is detected by user discovery, rather than reported by an User Agent. The system 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. In this case, the Defense Center regularly queries the LDAP server to obtain new and updated metadata for users whose activity the system detected since the last query.

For more information, see:
- Connecting to an LDAP Server for User Awareness and Control, page 17-4
- Updating User Control Parameters On-Demand, page 17-8
- Pausing Communications with an LDAP Server, page 17-9

Connecting to an LDAP Server for User Awareness and Control

License: FireSIGHT or Control
Supported Devices: feature dependent
Supported Defense Centers: feature dependent

Connections between Defense Centers and your organization’s LDAP servers can:
- specify the access-controlled users and groups whose activity you want to monitor with User Agents, and who you can use as criteria when limiting traffic with access control rules
- allow you to query the server for metadata on access-controlled users, as well as some non-access-controlled users: POP3 and IMAP users detected by user discovery and LDAP users whose activity is detected by either user discovery or a User Agent.

These connections, or user awareness objects, specify connection settings and authentication filter settings for the LDAP server. They are similar to the authentication objects you configure to manage external authentication to the FireSIGHT System’s web interface; see Managing Authentication Objects, page 61-5.
To perform user control, you **must** connect to a Microsoft Active Directory LDAP server. If you simply want to retrieve LDAP user metadata, the system supports connections to other types of LDAP server; see Table 17-1 on page 17-2.

When the system detects user activity, it can add a record of that user to the Defense Center users database, also called the user identity database. The Defense Center regularly queries the LDAP server to obtain metadata for new and updated users whose activity was detected since the last query. If a user already exists in the database, the system updates the metadata if it has not been updated in the last 12 hours. It may take several minutes for the Defense Center to update with user metadata after the system detects a new user login.

The system uses the email addresses in POP3 and IMAP logins to correlate with users on the LDAP server. For example, if a managed device detects a POP3 login for a user with the same email address as an LDAP user, the system associates the LDAP user’s metadata with that user.

**Note**

If you remove a user that has been detected by the system from your LDAP servers, the Defense Center 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 Defense Center next updates its list of access-controlled users.

The following table lists the LDAP metadata you can associate with monitored users. Note that to successfully retrieve user metadata from an LDAP server, the server **must** use the LDAP field names listed in the table. If you rename the field on the LDAP server, the Defense Center cannot populate its database with the information in that field.

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Defense Center</th>
<th>Active Directory</th>
<th>Oracle Directory Server</th>
<th>OpenLDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP user name</td>
<td>Username</td>
<td>samaccountname</td>
<td>cn</td>
<td>cn</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>uid</td>
<td>uid</td>
</tr>
<tr>
<td>first name</td>
<td>First Name</td>
<td>givenname</td>
<td>givenname</td>
<td>givenname</td>
</tr>
<tr>
<td>last name</td>
<td>Last Name</td>
<td>sn</td>
<td>sn</td>
<td>sn</td>
</tr>
<tr>
<td>email address</td>
<td>Email</td>
<td>mail</td>
<td>userprincipalname (if</td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>mail has no value)</td>
<td></td>
</tr>
<tr>
<td>department</td>
<td>Department</td>
<td>department</td>
<td>department</td>
<td>ou</td>
</tr>
<tr>
<td></td>
<td></td>
<td>distinguishedname (if department has no value)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>telephone number</td>
<td>Phone</td>
<td>telephonenumber</td>
<td>n/a</td>
<td>telephonenumber</td>
</tr>
</tbody>
</table>

Work closely with your LDAP administrators to ensure your LDAP servers are correctly configured and that you can connect to them, and to obtain the information you must provide when creating an LDAP connection.

**Server Type, IP Address, and Port**

You must specify the server type, IP address or hostname, and port for a primary, and optionally a backup, LDAP server. To perform user control, you **must** use a Microsoft Active Directory server.
Chapter 17  Controlling Traffic Based on Users

Retrieving Access-Controlled Users and LDAP User Metadata

LDAP-Specific Parameters

When the Defense Center searches the LDAP server to retrieve user information on the authentication server, it needs a starting point for that search. You can specify the namespace, or directory tree, to search by providing a base distinguished name, or base DN. 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. Note that after you identify a primary server, you can automatically retrieve a list of available base DNs from the server and select the appropriate base DN.

You must supply user credentials for a user with appropriate rights to the user information you want to retrieve. Remember that the distinguished name for the user you specify must be unique to the directory information tree for the directory server.

You can also specify an encryption method for the LDAP connection. Note that if you are using a certificate to authenticate, the name of the LDAP server in the certificate must match the host name that you specified in the Defense Center web interface. For example, if you use 10.10.10.250 when configuring the LDAP connection but computer1.example.com in the certificate, the connection fails.

Finally, you must specify the timeout period after which attempts to contact an unresponsive LDAP server roll over to the backup connection.

User and Group Access Control Parameters

To perform user control, specify the groups you want to use as criteria in access control rules.

Including a group automatically includes all of that group’s members, including members of any sub-groups. However, if you want to use the sub-group in access control rules, you must explicitly include the sub-group. You can also exclude groups and individual users. Excluding a group excludes all the members of that group, even if the users are members of an included group.

The maximum number of users you can use in access control depends on your FireSIGHT license. When choosing which users and groups to include, make sure the total number of users is less than your FireSIGHT user license. If your access control parameters are too broad, the Defense Center 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 do not specify any groups to include, the system retrieves user data for all the groups that match the LDAP 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. Note that you cannot include the Users or Domain Users groups.

You must also specify how often the Defense Center queries the LDAP server to obtain new users to use in access control.

After you create an LDAP connection, you can delete it by clicking the delete icon ( ) and confirming your choice. To modify an LDAP connection, click the edit icon ( ). If the connection is enabled, your saved changes take effect when the Defense Center next queries the LDAP server.

To create an LDAP connection for user awareness or user control:

Access: Admin/Discovery Admin

Step 1  Select Policies > Users.

The Users Policy page appears.
Step 2  Click **Add LDAP Connection**.

The Create User Awareness Authentication Object page appears.

Step 3  Type a **Name** and **Description** for the object.

Step 4  Select the LDAP **Server Type**.

If you want to perform user control, you **must** use a Microsoft Active Directory server.

**Note**

User Agents cannot transmit Active Directory user names ending with the $ character to the Defense Center. You must remove the final $ character if you want to monitor these users.

Step 5  Specify an **IP Address** or **Host Name** for a primary and, optionally, a backup LDAP server.

Step 6  Specify the **Port** that your LDAP servers use for authentication traffic.

Step 7  Specify the **Base DN** for the LDAP directory you want to access.

For example, to authenticate names in the Security organization at the Example company, type `ou=security,dc=example,dc=com`.

**Tip**

To fetch a list of all available domains, click **Fetch DNs** and select the appropriate base distinguished name from the drop-down list.

Step 8  Specify the distinguished **User Name** and **Password** that you want to use to validate access to the LDAP directory. Confirm the password.

For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute and the object for the administrator in the Security division at our example company has a `uid` value of `NetworkAdmin`, you would type `uid=NetworkAdmin,ou=security,dc=example,dc=com`.

Step 9  Choose an **Encryption** method. If you are using encryption, you can add an **SSL Certificate**.

The host name in the certificate **must** match the host name of the LDAP server you specified in step 5.

Step 10  Specify the **Timeout** period (in seconds) timeout period after which attempts to contact an unresponsive primary LDAP server roll over to the backup connection.

Step 11  Optionally, before you specify user awareness settings for the object, test the connection by clicking **Test**.

Step 12  You have two options, depending on the type of LDAP server you selected in step 4:

- If you are connecting to an Active Directory server, you can enable **User/Group Access Control Parameters** to specify users to use in access control. Continue with the next step.

- If you are connecting to any other kind of server, or do not want to perform user control, skip to step 17.

Step 13  Click **Fetch Groups** to populate the available groups list using the LDAP parameters you provided.

Step 14  Specify the users you want to use in access control by using the right and left arrow buttons to include and exclude groups.

Including a group automatically includes all of that group’s members, including members of any sub-groups. However, if you want to use the sub-group in access control rules, you must explicitly include the sub-group. Excluding a group excludes all the members of that group, even if the users are members of an included group.

Step 15  Specify any particular **User Exclusions**.
Excluding a user prevents you from writing an access control rule using that user as a condition. Separate multiple users with commas. You can also use an asterisk (*) as a wildcard character in this field.

**Step 16** Specify how often you want to query the LDAP server to obtain new user and group information.

By default, the Defense Center queries the server once a day at midnight:

- Use the **Start At** drop-down list to specify when you want the query to occur. 0 represents midnight, 1 represents 1:00 AM, and so on.
- Use the **Update Interval** drop-down list to specify how often, in hours, you want to query the server.

**Step 17** Click **Save**.

If you added or made changes to user and group access control parameters, confirm that you want to implement your changes. The object is saved and the Users Policy page appears again.

**Step 18** Enable the connection by clicking the slider next to the connection you just created.

If you are enabling the connection and your connection has user and group access control parameters, choose whether you want to immediately query the LDAP server to obtain user and group information. Note that if you do not immediately query the LDAP server, the query occurs at the scheduled time. You can monitor any query’s progress in the task queue (**System > Monitoring > Task Status**).

---

**Updating User Control Parameters On-Demand**

**License:** Control

**Supported Devices:** Any except Series 2 or X-Series

**Supported Defense Centers:** Any except DC500

If you change the user and group access control parameters in an LDAP connection, or if you change the users or groups on your LDAP server and want your changes to be immediately available for user control, you can force the Defense Center to perform an on-demand user data retrieval from the Active Directory server.

The maximum number of users the Defense Center can retrieve from the server depends on your FireSIGHT license. If the access control parameters in your LDAP connection are too broad, the Defense Center obtains information on as many users as it can and reports the number of users it failed to retrieve in the task queue.

**To perform an on-demand user data retrieval:**

**Access:** Admin/Discovery Admin

**Step 1** Select **Policies > Users**.

The Users Policy page appears.

**Step 2** Next to the LDAP connection you want to use to query the LDAP server, click the download icon ( ).

The query begins. You can monitor its progress in the task queue (**System > Monitoring > Task Status**).
Pausing Communications with an LDAP Server

License: FireSIGHT or Control  
Supported Devices: feature dependent  
Supported Defense Centers: feature dependent

Only enabled LDAP connections allow the Defense Center to query LDAP servers. To stop queries, you can temporarily disable LDAP connections rather than deleting them.

When you re-enable an LDAP connection used for access control, you can force the Defense Center to query the server immediately for updated user and group information, or you can wait until the first scheduled query occurs.

To disable or re-enable an LDAP connection:  
Access: Admin/Discovery Admin

Step 1 Select Policies > Users.  
The Users Policy page appears.

Step 2 Pause or re-enable the connection by clicking the slider next to the connection you just created.

If you are re-enabling the connection and your connection has user and group access control parameters, choose whether you want to immediately query the LDAP server to obtain user and group information. If you do not immediately query the LDAP server, the query occurs at the scheduled time. You can monitor any query’s progress in the task queue (System > Monitoring > Task Status).

Using User Agents to Report Active Directory Logins

License: FireSIGHT

User Agents deployed on Microsoft Windows computers can monitor Microsoft Active Directory servers, then notify the Defense Center when LDAP users in your organization log in and out of hosts, or authenticate with Active Directory credentials for other reasons. For example, your organization may use services or applications that rely on Active Directory for centralized authentication.

This agent-reported information serves not only as a record of user activity in your organizations, but also as the basis of user control. For traffic to match an access control rule with a user condition, the IP address of either the source or destination host in the monitored session must be associated with a logged in access-controlled user. You can control traffic based on individual users or the groups those users belong to.

Note

If you want to perform user control, you must install and use User Agents. However, User Agents only report user activity related to Active Directory authentications. User awareness allows you to view all agent-reported user activity, as well as additional activity detected in allowed network traffic by managed devices. The system uses the discovery feature to identify login attempts over various protocols: AIM, IMAP, LDAP, Oracle, POP3, SIP, FTP, HTTP, and MDNS. For more information, see Understanding User Data Collection, page 45-3.
To retrieve LDAP user authentication records with User Agents for either user awareness or control, first configure each Defense Center to allow connections from the agents. In a high availability deployment, enable agent communications on both the primary Defense Center and the secondary Defense Center. User Agents can connect to up to five Defense Centers at a time. After you enable User Agent communications on the Defense Center, you can install agents on Windows computers; see Table 17-1 on page 17-2.

Finally, configure User Agents to receive data from Microsoft Active Directory servers and report the information to Defense Centers. You can also configure agents to exclude specific user names and IP addresses from the reporting, and log status messages to a local event log or the Windows application log. The User Agent Status Monitor health module monitors agents connected to a Defense Center; see Configuring User Agent Status Monitoring, page 68-27.

To configure the Defense Center to connect to a User Agent:

Access: Admin/Discovery Admin

Step 1 Select Policies > Users.

The Users Policy page appears.

Step 2 Click Add User Agent.

The Add User Agent pop-up window appears.

Step 3 Type a Name for the agent.

Step 4 Type the Hostname or Address of the computer where you plan to install the agent. You must use an IPv4 address; you cannot configure the Defense Center to connect to a User Agent using an IPv6 address.

Step 5 Click Add User Agent.

The Defense Center can now connect to a User Agent on the computer you specified. To delete the connection, click the delete icon ( ) and confirm that you want to delete it.

Step 6 Install User Agent on the computer you specified. Configure it to receive data from Microsoft Active Directory servers and report the information to Defense Centers.

For detailed, up-to-date information, see the User Agent Configuration Guide.