Control Users with the User Agent

The following topics discuss how to perform user awareness and user control with the user agent:

The User Agent Identity Source

The Cisco Firepower User Agent is a passive authentication method; it is an authoritative identity source, meaning user information is supplied by a trusted Active Directory server. When integrated with the Firepower System, the user agent monitors users when they log in and out of hosts with Active Directory credentials. The data gained from the User Agent can be used for user awareness and user control.

The user agent associates each user with an IP address, which allows access control rules with user conditions to trigger. You can use one user agent to monitor user activity on up to five Active Directory servers and send encrypted data to up to five Firepower Management Centers.

The User Agent does not report failed login attempts.

Video User agent setup video on YouTube.

End of FMC Support for User Agent

End of support is planned for FMC integration with the Cisco Firepower User Agent (hereafter referred to as *user agent*) in a future release.

We strongly recommend you stop using the user agent and switch to using ISE/ISE-PIC as soon as possible.

You'll benefit from the following features, which are not available in the user agent:

- Support for Microsoft Active Directory up to version 2016
- Gathers authentication data from up to 10 Microsoft Active Directory domain controllers
- Gathers Active Directory authentication data from switches supporting Kerberos SPAN

- Supports passive/active redundancy
- You can upgrade from the ISE-PIC to ISE, adding the Passive Identity Connector node to an existing Cisco ISE cluster.
- Supports KVM, VMware, and Hyper-V
- Tailored to fit your organization with support for 3,000 and 300,000 sessions, depending on licensing

You are eligible for a free ISE-PIC license if you have a current support contract for any of the following:

- Any FMC hardware model
- Virtual FMC v25
- Virtual FMC v300

For the preceding models, request part number **L-FMC-ISE-PIC=**.

Note If you have FMCv2 and FMCv10, you must use the standard ISE-PIC part numbers.

Requirements and Prerequisites for User Agent

Model Support

Any.

Supported Domains

Global

User Roles

- Admin
- Access Admin
- Network Admin

User Agent Guidelines

The User Agent requires a multi-step configuration that includes the following:

- At least one computer with the user agent installed.
- Connections between a Firepower Management Center and the computers or Active Directory servers with the user agent installed.
- An identity realm configured in each Firepower Management Center that receives user data from a user agent.

For detailed information about the multi-step User Agent configuration and a complete discussion of the server requirements, see the *Cisco Firepower User Agent Configuration Guide*.

Note Make sure the time on your computer or Active Directory server is synchronized with the time on the Firepower Management Center. If the appliances are not synchronized, the system might perform user timeouts at unexpected intervals.

The Firepower Management Center connection not only allows you to retrieve metadata for the users whose logins and logoffs were detected by User Agents, but also is used to specify the users and groups you want to use in access control rules. If the user agent is configured to exclude specific user names, login data for those user names are not reported to the Firepower Management Center. User agent data is stored in the user database and user activity database on the Firepower Management Center.

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

If multiple users are logged into a host using remote sessions, the agent might not detect logins from that host properly. For information about how to prevent this, see the *Cisco Firepower User Agent Configuration Guide*.

Configure the User Agent for User Control

For more information about the User Agent, see The User Agent Identity Source, on page 1.

Before you begin

- Configure and enable an Active Directory realm for your User Agent connection as described in Create a Realm.

Step 1 Log in to the Firepower Management Center.

Step 2 Click **System** > **Integration**.

Step 3 Click **Identity Sources**.

Step 4 Click **User Agent** for the **Service Type** to enable the User Agent connection.

Note To disable the connection, click **None**.

Step 5 Click **New Agent** to add a new agent.

Step 6 Enter the **Hostname** or **Address** of the computer where you plan to install the agent. You must use an IPv4 address; you cannot configure the Firepower Management Center to connect to a User Agent using an IPv6 address.

Step 7 Click **Add**.

Step 8 To delete a connection, click **Delete** () and confirm that you want to delete it.

What to do next

- Continue User Agent setup as described in the *Cisco Firepower User Agent Configuration Guide*.
- Configure an identity rule as described in Create an Identity Rule.
- Associate the identity policy with an access control policy as discussed in Associating Other Policies with Access Control.
- Deploy your identity and access control policies to managed devices as discussed in Deploy Configuration Changes.

Related Topics

Troubleshoot the User Agent Identity Source, on page 4
Access Control Policies

Troubleshoot the User Agent Identity Source

If you experience issues with the User Agent connection, see the *Cisco Firepower User Agent Configuration Guide*.

For related troubleshooting information in this guide, see Troubleshoot Realms and User Downloads and Troubleshoot User Control.

If you experience issues with user data reported by the User Agent, note:

- After the system detects activity from a User Agent user whose data is not yet in the database, the system retrieves information about them from the server. That user's activity is not handled by rules, and is not displayed in the web interface until the system successfully retrieves information about them in a user download.
- If you have Firepower Management Center high availability configured and the primary fails, all logins reported by a User Agent cannot be identified during failover downtime, even if the users were previously seen and downloaded to the Firepower Management Center. The unidentified users are logged as Unknown users on the Firepower Management Center. After the downtime, the Unknown users are re identified and processed according to the rules in your identity policy.
- If the User Agent monitors the same users as the TS Agent, the system prioritizes the TS Agent data. If the TS Agent and the User Agent report identical activity from the same IP address, only the TS Agent data is logged.
- Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, see RFC 959.

History for the User Agent

Feature	Version	Details
User agent deprecated	6.5	The user agent is deprecated and will be removed in a future release. We strongly recommend you use ISE/ISE-PIC instead of the user agent.
User agent version 2.5	6.5	You can change the default password the user agent uses to authenticate with the FMC. New FMC command: **configure user-agent**
User agent for user control.	—	Feature introduced before Version 6.0. User agent provides login details for Active Directory users and can be used for user awareness and user control.