Introduction to the User Agent

Version 2.5 of the user agent work in conjunction with version 6.4 or later of the Firepower System managed devices to gather user data. The user agent is also essential to implementing user access control.

A user agent monitors up to five Microsoft Active Directory servers and reports logins and logoffs authenticated by Active Directory. The Firepower System integrates these records with the information it collects using traffic-based detection on managed devices.

Caution The user agent is reaching its end of support period. Firepower Management Center version 6.6 is the last version with which you can enable the user agent. The user agent cannot be enabled in Firepower Management Center 6.7 and upgrades to 6.7 will warn you to disable the user agent before upgrading.

You must migrate to the Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) before you upgrade to FMC version 6.7.

For more information, see End of FMC Support for the User Agent, page 1-6.

Note Version 2.5 of the user agent works only with the Firepower Management Center version 6.4 or later. If you have issues with the user agent and your version of the Firepower Management Center, you can replace the version 2.5 user agent with an earlier user agent version as discussed in Troubleshoot the User Agent, page 2-34.

About the User Agent

This section discusses the role of the user agent in implementing user discovery on the Firepower System. For a more detailed discussion of all concepts related to user discovery, network discovery, and identity sources, see the configuration guide for your system.

For more information, see the following sections:

User Agent Fundamentals

The Firepower System can obtain both user identity and user activity information from your organization's Active Directory servers. The user agent enables you to monitor users when users authenticate with Microsoft Active Directory servers.

Note To perform user control, your organization *must* use Microsoft Active Directory. The Firepower System uses user agents that monitor Active Directory servers to associate users with IP addresses, which is what allows access control rules to trigger.

Installing and using the user agent enables you to perform user control; the agent associates a user name with one or more IP addresses, and this information can trigger access control rules with user conditions.

A complete user agent configuration for user control includes the following:

- A computer with the agent installed.
- A connection between a Management Center and the user agent computer.
- A connection between each Management Center to the monitored Active Directory servers.
- This version of the user agent is supported by Firepower Management Center 6.2.3 and later.

For more information about user control, see the configuration guide for your system.

You can install the user agent on any Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows Server 2008, or Microsoft Windows Server 2012 computer with TCP/IP access to the Microsoft Active Directory servers to monitor. You can also install the agent on an Active Directory server running one of the supported operating systems; however, doing so is less secure.

Note If you install the user agent on Windows Server 2003 or an older operating system, the user agent cannot collect real time statistics from an Active Directory computer.

The Management Center connection not only enables 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 agent is configured to exclude specific user names, login data for those user names are not reported to the Management Center.

Agent Monitoring, Polling, and Reporting

Each user agent can monitor authoritative logins using encrypted traffic by either regularly scheduled polling or real time monitoring.

The following are among the events the user agent reports to the Management Center:

- **User Login**: A user logs in to a computer with an IP address not associated with the user name the last time the user was seen.

  In other words, suppose user name `james.harvey` logs in to IP address 192.0.2.100 on Monday. On Tuesday, `james.harvey` logs in to IP address 192.0.2.105. This login triggers a User Login event in the Management Center.

  User Login events occur whether the user logs in directly to a workstation or uses Remote Desktop.

- **User Logoff**: Occurs when a user logs out of an IP address. User Logoff events are reported to the management center at a configurable interval, not immediately after a user logs off of a computer.

- **New User Identity**: One-time event that occurs the first time a user name is associated with an IP address.
- **Delete User Identity**: Occurs after a Management Center administrator deletes a user identity.

Combining logoff data with login data develops a more complete view of the users logged into the network.

Polling an Active Directory server enables an agent to retrieve batches of user activity data at the defined polling interval. Real time monitoring transmits user activity data to the agent as soon as the Active Directory server receives the data.

You can configure the agent to exclude reporting any logins or logoffs associated with a specific username or IP address. This can be useful, for example, to exclude repeated logins to the following:

- Shared servers, such as file shares and print servers
- The user agent computer
- The Active Directory server
- Logins into computers for troubleshooting purposes

You can configure an agent to monitor up to five Active Directory servers and to send encrypted data on to as many as five Management Centers.

If you are using version 6.2.3 or later to perform access control, the logins reported by user agents associate users with IP addresses, which in turn allows access control rules with user conditions to trigger.

Note If multiple users are logged into a host using remote sessions, the agent might not detect logins from that host properly. See Enable Idle Session Timeouts, page 2-5 for more information on how to prevent this.

Table 1-1 Polling and Monitoring Notes

Concept	Notes
Login detection	The agent reports user logins to hosts with IPv6 addresses to Firepower Management Center running Version 6.2.3 or later. The agent reports non authoritative user logins and NetBIOS logins to Firepower Management Center running Version 6.2.3 or later. To detect logins to an Active Directory server, you must configure the Active Directory server connection with the server IP address. See Configure User Agent Active Directory Server Connections, page 2-23 for more information.
Logoff detection	The agent reports detected logoffs to Firepower Management Center version 6.2.3 or later. Logoffs might not be immediately detected. The timestamp associated with a logoff is the time the agent detected the user was no longer mapped to the host IP address, which might not correspond with the time the user logged off of the host.
Real Time data retrieval	The Active Directory server must run Windows Server 2008 or Windows Server 2012. The user agent computer must run Windows 7, Windows 8, Windows 10, or a Windows Server version more recent than Server 2003.

User Agent Login Data

The user agent monitors users as they log in to the network or when accounts authenticate against Active Directory credentials for other reasons. The user agent detects interactive user logins to a host, Remote Desktop logins, file-share authentication, and computer account logins.

User agents report *authoritative* user logins. Authoritative login data (for example, a remote desktop login or an interactive login to a host by a user) causes the current user mapped to the host IP address to change to the user from the new login.

Network discovery traffic-based detection reports *non authoritative* user logins. Non-authoritative logins either do not change the current user or change the current user only if the user was also non-authoritative.

Note, however, the following caveats:

- If the agent detects a login for file-share authentication, the agent reports a user login for the host, but does not change the current user on the host.
- If the agent detects a computer account login to a host, the agent generates a NetBIOS Name Change discovery event and the host profile reflects any change to the NetBIOS name.
- If the agent detects a login from an excluded user name, the agent does not report a login to the Management Center.

For all logins, the agent sends the following information to the Management Center:

- The user's LDAP user name

Note The Management Center might not correctly display user names with Unicode characters.

- The time of the login or other authentication
- The IP address of the user's host, and the link-local address if the agent reports an IPv6 address for a computer account login

Note If a user uses a Linux computer to log in using Remote Desktop to a Windows computer, after the agent detects the login, it reports the Windows computer's IP address, not the Linux computer's IP address, to the Management Center.

The Management Center records login and logoff information in the user activity database and user data in the user database. When a user agent reports user data from a user login or logoff, the reported user is checked against the list of users in the users database. If the reported user matches an existing user reported by an agent, the reported data is assigned to the user. Reported users that do not match existing users cause a new user to be created.

Even though the user activity associated with an excluded user name is not reported, related user activity might still be reported. If the agent detects a user login to a computer, then the agent detects a second user login, and you have excluded the user name associated with the second user login from reporting, the agent reports a logoff for the original user. However, no login for the second user is reported. As a result, no user is mapped to the IP address, even though the excluded user is logged into the host.

Note the following limitations on user names detected by the agent:

- User names ending with a dollar sign character are not reported to any other versions of Management Centers.
- Management Center display of user names containing Unicode characters might have limitations.

The total number of detected users the Management Center can store depends on the following:

- In Version 6.x, your Management Center model

After you reach the user limit, in most cases the system stops adding new users to the database. To add new users, you must either manually delete old or inactive users from the database, or delete all users from the database.

Deploy Multiple User Agents

If you have more than one Active Directory server per domain, you can consider installing more than one user agent. Active Directory servers share authentication information but not their security logs, which is where the user agent gathers some of its information.

Therefore, if there is more than one Active Directory server in your domain, you can either:

- Install one user agent that communicates with more than one Active Directory server.

  One user agent can communicate with up to five Active Directory servers.

- Install more than one user agent, each of which communicates with a different Active Directory server or domain controller.

  We recommend this type of deployment in the following circumstances:

  - Active Directory servers are geographically dispersed; we recommend installing user agents on computers that are geographically proximate to the Active Directory server (or on the Active Directory server computer itself, although this is less secure).
  - Active Directory servers are heavily loaded with traffic.

Note You must configure each user agent to communicate with the fully qualified hostname or IP address of the domain controller. In a multi-domain system, it's common for each domain controller to have a different IP address or hostname.

Legacy Agent Support

Version 1.0 (legacy) user agents installed on Active Directory servers can continue to send user login data from the Active Directory server to a single Management Center. Deployment requirements and detection capabilities of legacy agents are unchanged.

You must install legacy agents on the Active Directory server to connect to exactly one Management Center. Note, however, that the User Agent Status Monitor health module does not support legacy agents and should not be enabled on Management Centers with legacy agents connected.

You should plan to upgrade your deployment to use Version 2.5 of the user agent as soon as possible in preparation for future releases when support for legacy agents will be phased out.

About the User Agent, ISE, and Access Control in Version 6.x

Version 6.0 introduced support for the Cisco Identity Services Engine (ISE), an alternative to the user agent. The user agent and ISE are passive identity sources that gather data for user access control. To perform user control in Version 6.x, you must configure an identity realm for your monitored Active Directory servers on the Management Center connected to the agent or ISE device. For more information about realms, identity sources, and ISE/ISE-PIC, see the configuration guide for your system.

End of FMC Support for the User Agent

Firepower Management Center version 6.6 is the last version with which you can enable the user agent. The user agent cannot be enabled in Firepower Management Center 6.7 and upgrades to 6.7 will warn you to disable the user agent before upgrading.

We strongly recommend you stop using the user agent and switch to using the Cisco Identity Services Engine/Passive Identity Connector (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=`.

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

For more information, see End-of-Life and End-of-Support for the Cisco Firepower User Agent.

Fixed Issues in This Release

The following issues were fixed in this release:

Caveat ID Number	Description
CSCvo61952	User agent version 2.4 can communicate with ASA with FirePOWER Services devices after upgrading to version 6.3.
CSCvo24540	User agent version 2.4 has upgraded its Microsoft SQL Server Compact Edition support to address vulnerabilities.
CSCvo08211	Version 2.5 of the user agent enables you to set a password for authenticating the user agent with the Firepower Management System. To use the default password, no action is required. To set a password, you must do all of the following: • Use the `configure user-agent` command on the Firepower Management Center (not a managed device) to create a password. For more information, see the chapter on the Firepower Management Center CLI Reference in the *Firepower Management Center Configuration Guide*. • Set the same password in the user agent and restart the user agent service. For more information, see Change the User Agent Password, page 2-27.