User Control with TS Agent

To use the TS Agent as an identity source for user awareness and user control, install and configure the TS Agent software as discussed in the Cisco Terminal Services (TS) Agent Guide.

What to do next:

- Specify users to control and other options using an identity policy as described in Create an Identity Policy.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, 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.
- Monitor user activity as discussed in *Using Workflows* in the Cisco Secure Firewall Management Center Administration Guide .

The Terminal Services (TS) Agent Identity Source

The TS Agent is a passive authentication method and one of the authoritative identity sources supported by the system. A Windows Terminal Server performs the authentication, and the TS Agent reports it to a standalone or high availability Firewall Management Center.

When installed on Windows Terminal Servers, the TS Agent assigns a unique port range to individual users as they log in or log out of a monitored network. The Firewall Management Center uses the unique port to identify individual users in the system. You can use one TS Agent to monitor user activity on one Windows Terminal Server and send encrypted data to a Firewall Management Center.

The TS Agent does not report failed login attempts. The data gained from the TS Agent can be used for user awareness and user control.

TS Agent Guidelines

The TS Agent requires a multi-step configuration, and includes the following:

1. A Windows Terminal Server with the TS Agent installed and configured.
2. One or more identity realms targeting the users your server is monitoring.

You install the TS Agent on a Microsoft Windows Terminal Server. For detailed information about the multi-step TS Agent installation and configuration and a complete discussion of the server and system requirements, see the Cisco Terminal Services (TS) Agent Guide.

TS Agent data is visible in the Users, User Activity, and Connection Event tables and can be used for user awareness and user control.

Note If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and another passive identity source report activity by the same IP address, only the TS Agent data is logged to the Firewall Management Center.

User Control with TS Agent

To use the TS Agent as an identity source for user awareness and user control, install and configure the TS Agent software as discussed in the Cisco Terminal Services (TS) Agent Guide.

What to do next:

- Specify users to control and other options using an identity policy as described in Create an Identity Policy.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, 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.
- Monitor user activity as discussed in *Using Workflows* in the Cisco Secure Firewall Management Center Administration Guide .

Troubleshoot the TS Agent Identity Source

For other related troubleshooting information, see Troubleshoot Realms and User Downloads and Troubleshoot User Control.

If you experience issues with the TS Agent integration, check:

- You must synchronize the time on your TS Agent server with the time on the Firewall Management Center.

- If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Firewall Management Center prioritizes the TS Agent data. If the TS Agent and a passive identity source report activity by the same IP address, only the TS Agent data is logged to the Firewall Management Center.
- 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.

For more troubleshooting information, see the Cisco Terminal Services (TS) Agent Guide.

History for TS Agent

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
TS Agent for user control.	7.2.0	6.2.0	Feature introduced. Firepower now provides the ability to better identify individual users in shared environments, such as Citrix's Virtual Desktop Infrastructure (VDI), to accurately enforce user-based policy rules on the firewall. Users are identified by ports used. The TS Agent software is updated independently of the Firepower Management Center. For more information, see: • *Cisco Terminal Services (TS) Agent Guide* available on cisco.com • Cisco Firepower Compatibility Guide