

Identity source: 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 Terminal Services (TS) Agent guides.

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 Associate prefilter, decryption, and identity policies with an access control.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes.
- Monitor user activity.

- Terminal services agent identity source, on page 1
- Best practices for TS agent configuration, on page 2
- Identity source: TS agent, on page 2
- Troubleshoot the TS agent identity source, on page 2
- History for TS agent, on page 3

Terminal services 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 .

TS agent functionality

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 Cloud-Delivered 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 Cloud-Delivered 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.

Best practices for TS agent configuration

Configure the TS Agent on a Windows Terminal Server to monitor user activity and identity realms. The TS Agent enables user awareness in the Cloud-Delivered Firewall Management Center.

- Install and configure the TS Agent on a Windows Terminal Server.
- Configure one or more identity realms targeting the users your server is monitoring.

TS Agent data is visible in the Users, User Activity, and Connection Event tables and can be used for user awareness and user control. For detailed information about the multi-step TS Agent installation and configuration and a complete discussion of the server and system requirements, see the Terminal Services (TS) Agent guides.

Note If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Cloud-Delivered 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 Cloud-Delivered Firewall Management Center.

Identity source: 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 Terminal Services (TS) Agent guides.

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 Associate prefilter, decryption, and identity policies with an access control.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes.
- Monitor user activity.

Troubleshoot the TS agent identity source

This reference provides troubleshooting guidance for TS Agent integration issues with the Cloud-Delivered Firewall Management Center. It addresses synchronization requirements, user data prioritization, and activity logging for overlapping passive identity sources.

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 Cloud-Delivered Firewall Management Center.
- If the TS Agent monitors the same users as another passive authentication identity source (ISE/ISE-PIC), the Cloud-Delivered 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 Cloud-Delivered 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, refer to RFC 959.

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

History for TS agent

This reference provides the historical development timeline and version information for the TS Agent feature, including compatibility details and feature introductions across different Firepower Management Center and Threat Defense versions.

Feature	Minimum Cloud-Delivered Firewall Management Center	Minimum Firewall Threat Defense	Details
TS Agent communicates with the Security Cloud Control	Any	7.2.0	By applying a token from Security Cloud Control, the TS Agent can get user login sessions in the same way as for the Security Cloud Control.
TS Agent for user control.	Any	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