Introduction to the Terminal Services (TS) Agent

About the Cisco Terminal Services (TS) Agent

The Cisco Terminal Services (TS) Agent allows the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC to uniquely identify user traffic monitored by a Microsoft Windows Terminal Server. Without the TS Agent, the systems recognize all traffic from a Microsoft Windows Terminal Server as one user session originating from one IP address.

The TS Agent can be used with all of the following:

- The Cloud-delivered Firewall Management Center available with the Cisco Defense Orchestrator (CDO).

- The On-Prem Firewall Management CenterFMC available with CDO.

- A standalone Management Center or high availability system that is not associated with CDO.

For brevity, in this guide, unless otherwise noted, *On-Prem Firewall Management CenterFMC* can mean either a Management Center associated with CDO or a standalone system that is not associated with CDO.

✎

Note To avoid potential issues and to make sure you're using the most up-to-date software, Cisco recommends using the latest released version of the TS Agent. To find the latest version, go to the Cisco Support site.

When installed and configured on your Microsoft Windows Terminal Server, the TS Agent assigns a port range to individual user sessions, and ports in that range to the TCP and UDP connections in the user session. The systems use the unique ports to identify individual TCP and UDP connections by users on the network. Port ranges are assigned on a least recently used basis, meaning that after a user session ends, the same port range is not immediately reused for new user sessions.

Note   ICMP messages are passed without port mapping.

Traffic generated by a service running in the computer's System context is not tracked by the TS Agent. In particular, the TS Agent does not identify Server Message Block (SMB) traffic because SMB traffic runs in the System context.

The TS Agent supports up to 199 simultaneous user sessions per TS Agent host. If a single user runs several simultaneous user sessions, the TS Agent assigns a unique port range to each individual user session. When a user ends a session, the TS Agent can use that port range for another user session.

Each Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC supports up to 50 TS Agents connecting to it at the same time.

There are three primary components to the TS Agent installed on your server:

  • Interface—application to configure the TS Agent and monitor the current user sessions

  • Service— program that monitors the user logins and logoffs

  • Driver— program that performs the port translation

The TS Agent can be used for the following:

  • TS Agent data on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC can be used for user awareness and user control. For more information about using TS Agent data in the Firepower System, see the *Firepower Management Center Configuration Guide*.

Note   To use TS Agent for user awareness and control, you must configure it to send data *only* to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. For more information, see Configure the TS Agent.

Server and System Environment Requirements

You must meet the following requirements to install and run the TS Agent on your system.

Note   To avoid potential issues and to make sure you're using the most up-to-date software, Cisco recommends using the latest released version of the TS Agent. To find the latest version, go to the Cisco Support site.

Server Requirements

Install the TS Agent on one of the following 64-bit Microsoft Windows Terminal Server versions:

  • Microsoft Windows Server 2019

  • Microsoft Windows Server 2016

  • Microsoft Windows Server 2012

Introduction to the Terminal Services (TS) Agent

Troubleshoot On-Prem Firewall Management CenterFMCIssues with the TS Agent

> • Microsoft Windows Server 2012 R2

TS Agent requires the following and installs them if they are not present:

> • Microsoft .NET Framework 4.6.2

> • Microsoft Visual C++ Update 4

Note The TS Agent installation requires 653KB of free space on your server.

Note If the TS Agent server uses anti-virus software that proxies web traffic, user traffic is typically assigned to the System user and the On-Prem Firewall Management CenterFMC or Cloud-delivered Firewall Management Center sees those users as Unknown. To avoid the issue, disable web traffic proxying.

The TS Agent is compatible with any of the following terminal services solutions installed on your server:

> • Citrix Provisioning

> • Citrix XenDesktop

> • Citrix XenApp

> • Xen Project Hypervisor

> • VMware vSphere Hypervisor/VMware ESXi 6.0

> • Windows Terminal Services/Windows Remote Desktop Services (RDS)

This version of the TS Agent supports using a single network interface controller (NIC) for port translation and server-system communications. If two or more valid NICs are present on your server, the TS Agent performs port translation only on the address you specify during configuration. A valid NIC must have a single IPv4 or IPv6 address, or one of each type; a valid NIC cannot have multiple addresses of the same type.

Note If router advertisements are enabled on any devices connected to your server, the devices can assign multiple IPv6 addresses to NICs on your server and invalidate the NICs for use with the TS Agent.

Troubleshoot On-Prem Firewall Management CenterFMCIssues with the TS Agent

On-Prem Firewall Management CenterFMC test connection fails

If you are logged in to the TS Agent server as a local user (as opposed to a domain user), the TS Agent test connection with the On-Prem Firewall Management CenterFMC test fails. This happens because, by default, the TS Agent does not allow System processes to communicate on the network.

Introduction to the Terminal Services (TS) Agent

3

To work around the issue, do any of the following:

- Check **Unknown Traffic Communication** on the **Configure** tab page to allow the traffic, as discussed in TS Agent Configuration Fields.

- Log in to the TS Agent computer as a domain user rather than as a local user.

TS Agent reports users as Unknown and rules not matched

If other vendors' Terminal Services agents are running on the same server as the Cisco Terminal Services (TS) Agent, port numbers for user connections might not be in the assigned User Ports range. As a result, users can be identified as Unknown and therefore identity rules do not match for users.

To resolve this issue, disable or uninstall the other Terminal Services agents running on the same server as the Cisco TS Agent.

TS Agent prompts to reboot on upgrade

Sometimes, even if the machine's IP address does not change, TS Agent reports an IP address change after upgrade and prompts you to reboot the server. This happens because the TS Agent detects a difference between the IP address and the value of the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TSAgent\{IPv4 | IPv6}`

If the key value is different from the configured primary adapter IP address, TS Agent reports the change and instructs you to save the configuration and reboot the computer.

This can happen, for example, if the computer was reimaged or restored from backup and DHCP assigns a new IP address.

You can ignore the error but you must reboot the computer after upgrading anyway.

Citrix Provisioniong clients fail to boot

You must configure the TS Agent to ignore the UDP port(s) you configured for the Citrix Provisioning server.

The value you specify in the TS Agent **Reserve Port(s)** field must match one of the Citrix Provisioning **First and Last UDP port numbers** ports.

⚠️

Caution   Failure to specify the correct port will cause clients to fail to boot.

Exceptions when saving the TS Agent IP address

In rare circumstances, exceptions are displayed when you attempt to save the TS Agent configuration with an invalid IP address. An invalid IP address can be any of the following:

- The same IP address as another device on the network.

- Changing the static IP address in Windows while the TS Agent application is open.

Exceptions include the following:

- `System.ArgumentException: An item with the same key has already been added.`

- `System.NullReferenceException: Object reference not set to an instance of an object.`

Workaround: Set the TS Agent server's IP address to a valid IP address, save the TS Agent configuration, and reboot the server.

Resolved Issues

Resolved Issues

Caveat ID Number	Description
CSCwc41073	Protocol errors communicating with the management center result in the TS Agent retrying the connection instead of failing.

History for TS Agent

Feature	Version
Supports both the On-Prem Firewall Management CenterFMC and Cloud-delivered Firewall Management Center available with the Cisco Defense Orchestrator, as well as a standalone Management Center.	1.4
• Added support for Citrix Provisioning • The value you specify in the TS Agent **Reserve Port(s)** field must match one of the Citrix Provisioning **First and Last UDP port numbers** ports. **Caution** Failure to specify the correct port will cause clients to fail to boot.	1.3

Feature	Version
• Detects an IP address change on the server, prompts you to save configuration and reboot. See TS Agent Configuration Fields. • Enables you to upgrade to this version without uninstalling the previous version. See Install or Upgrade the TS Agent. • Renamed **Exclude Port(s)** configuration field to **Reserve Port(s)**. See TS Agent Configuration Fields. • Support for ephemeral ports. See TS Agent Configuration Fields. • The **Monitor** tab page warns you when more than 50% percent of TCP or UDP ports have been used for a particular session. See View Information About the TS Agent. • User session port ranges assigned on least recently used basis. See About the Cisco Terminal Services (TS) Agent, on page 1. • Enables you to export troubleshooting information to an XML file. See View Information About the TS Agent. • Enables you to restream user sessions to the Management Center. See View Information About the TS Agent. • Attempts to end all user sessions when TS Agent is uninstalled. See Uninstalling the TS Agent.	1.2
• Default maximum number of max user sessions changed from 200 to 30. • Port range changed from 200 or more to 5000 or more These changes are all discussed in TS Agent Configuration Fields.	1.1
TS Agent Feature introduced. The TS Agent enables administrators to track user activity using port mapping. The TS Agent, when installed on a Terminal Server, assigns a port range to individual user sessions, and ports in that range to the TCP and UDP connections in the user session. The systems use the unique ports to identify individual TCP and UDP connections by users on the network.	1.0