Introduction to the Terminal Services Agent

About the Terminal Services (TS) Agent

The Cisco Terminal Services (TS) Agent allows the Firepower Management Center 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.

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 FMC 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 FMC can be used for user awareness and user control. For more information about using the TS Agent data in the System, see the *Cisco Secure Firewall Management Center Configuration Guide*.

Note To use TS Agent for user awareness and control, you must configure it to send data *only* to the FMC. 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 2016
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

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 FMC 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 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.

System Requirements

This version of the TS Agent supports connecting to standalone or high availability FMCs running Version 6.2 or later of the System.

Troubleshooting Firepower Management Center Issues with the TS Agent

See the following sections for information about troubleshooting Firepower Management Center issues with the TS Agent.

For information about known and fixed issues in this release, see Known Issues and Resolved Issues, on page 7.

FMC does not display user information for System processes

Traffic generated by a service running in the System context is not tracked by the TS Agent. In particular, note the following:

- The TS Agent does not identify Server Message Block (SMB) traffic because SMB traffic runs in the System context.
- Some anti-virus applications proxy web traffic to an on-premises or cloud gateway to catch viruses before they reach a client computer. However, this means that the anti-virus software typically uses the System account; in this case, the FMC sees the users as Unknown. To resolve the issue, disable web traffic proxying.

TS Agent user timeouts do not occur when expected

You must synchronize the time on your server with the time on the FMC.

TS Agent does not translate user session ports

The TS Agent does not perform port translation in the following cases:

- A user session exceeds the set **Max User Sessions** value. For example, if the **Max User Sessions** is set to 29, the TS Agent does not perform port translation on the 30th user session.
- All available ports are in use. For example, if your **User Ports Range** value designates 1000 ports per user session, the TS Agent does not perform port translation on the 1001st TCP/UDP connection until the user ends another TCP/UDP connection and releases a port.
- A user session does not have an associated domain. For example, if a server administrator's session is authenticated by the local system and not by an external Active Directory server, the server administrator logs in to the server but cannot access the network and the TS Agent does not assign ports to the user session.

User sessions are not reported to the FMC as expected

If you update the TS Agent configuration to connect to a different FMC, you must end all current user sessions before saving the new configuration. For more information, see Ending a Current User Session.

Client application traffic is reported to the FMC as user traffic

If there is a client application installed on your server and the application is configured to bind to a socket that uses a port that falls outside of your **System Ports**, you must use the **Exclude Port(s)** field to exclude that port from translation. If you do not exclude the port and it falls within your **User Ports**, the TS Agent may report traffic on that port as unrelated user traffic.

To prevent this, configure your client application to bind to a socket that uses a port that falls within your **System Ports**.

Server application timeout, browser timeout, or TS Agent-FMC connection failure

If an application on the TS Agent server ends a TCP/UDP connection but incompletely closes the associated port, the TS Agent cannot use that port for translation. If the TS Agent attempts to use the port for translation before the server closes the port completely, the connection fails.

Note You can use the `netstat` command (for summary information) or the `netstat -a -o -n -b` command (for detailed information) to identify incompletely closed ports; these ports have a state of `TIME_WAIT` or `CLOSE_WAIT`.

If you see this issue, increase the TS Agent port range affected by the issue:

- Server application or browser timeout occurs if an incorrectly closed port falls within the **User Ports** range.
- TS Agent-FMC connection failure occurs if an incorrectly closed port falls within the **System Ports** range.

TS Agent-FMC connection failure

If the TS Agent fails to establish a connection with the FMC when you click the **Test** button during configuration, check the following:

- Make sure no more than 50 TS Agent clients are attempting to connect to the FMC at the same time.
- Confirm that the **Username** and **Password** you provided are the correct credentials for a FMC user with REST VDI privileges as discussed in Creating the REST VDI Role.

  You can view the audit logs on the FMC to confirm that the user authentication from the TS Agent succeeded.
- If the connection to the secondary FMC in a high availability configuration fails immediately after configuration, this is expected behavior. The TS Agent communicates with the active FMC at all times.

  If the secondary is the active FMC, the connection to the primary FMC fails.

System processes or applications on the server are malfunctioning

If a system process on your server is using or listening in on a port that is not within your **System Ports** range, you must manually exclude that port using the **Exclude Port(s)** field.

If an application on your server is using or listening in on your Citrix MA Client (2598) or Windows Terminal Server (3389) port, confirm that those ports are excluded in the **Exclude Port(s)** field.

FMC shows Unknown users from the TS Agent

The FMC shows Unknown users from the TS Agent in the following situations:

- If the TS Agent driver component fails unexpectedly, user sessions seen during the downtime are logged as Unknown users on the FMC.
- Some anti-virus applications proxy web traffic to an on-premises or cloud gateway to catch viruses before they reach a client computer. However, this means that the anti-virus software typically uses the System account; in this case, the FMC sees the users as Unknown. To resolve the issue, disable web traffic proxying.
- If the primary FMC in a high availability configuration fails, logins reported by the TS Agent during the 10 minutes of downtime during failover are handled as follows:
  - If a user was not previously seen on the FMC and the TS Agent reports user session data, the data is logged as Unknown user activity on the FMC.
  - If the user was previously seen on the FMC, the data is processed normally.

  After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.

NICs are not displayed in the Server NIC list

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

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.

Troubleshoot Issues with the TS Agent

FMC 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 FMC test fails. This happens because, by default, the TS Agent does not allow System processes to communicate on the network.

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.

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.

Troubleshoot Issues with the User Agent

If you use both the TS Agent and the user agent, you can avoid non-critical errors in the logs by excluding the TS Agent IP address from the user agent. If the same user is detected by both the TS Agent and the user agent, non-critical errors are written to logs.

To prevent this, exclude the TS Agent's IP address from being logged by the user agent. For more information, see the *Firepower User Agent Configuration Guide*.

Known Issues and Resolved Issues

Known Issues

Caveat ID Number	Description
CSCvf63615	At log level 6, some incorrect function names are displayed in the logs.
CSCvf25546	When both IPv4 and IPv6 addresses are used on the TS Agent server, fewer mapping ports are available than expected.
CSCvf25342	If your Firepower Management Centers are configured as high availability and you specify connection information to a host name rather than an IP address, the TS Agent never connects to the new active system after failover.
CSCvf65188	In some cases, connections are not released when expected after a user logs out of the TS Agent server. Sometimes the TCP protocol allows a stale connection to persist longer than expected. This behavior can be confirmed by the following message in the Windows Event Log: `Event 4227: TCP/IP failed to establish an outgoing connection because the selected local endpoint was recently used to connect to the same remote endpoint.` **Workarounds**: • Increase the number of ports in the range. • Decrease the time TCP stack has to wait until such connections are fully released: `TcpTimedWaitDelay`, found in the following location in the Windows registry: `HKEY_LOCAL-MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters` For more information, see the description of `TcpTimedWaitDelay` on MSDN.

Resolved Issues

Caveat ID Number	Description
CSCvg65335	The TS Agent now notifies you when the server's IP address changes, after which you must save the change and reboot the server.
CSCvg65253	User IP bindings are now sent to the Firepower Management Center. As a result, the following error does *not* display on TS Agent event viewer log and the **Status** column on the TS Agent's **Monitor** tab page: **FMC_STATS_TO_BE_CONNECT**.

History for TS Agent

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 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 FMC. 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

Feature	Version
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