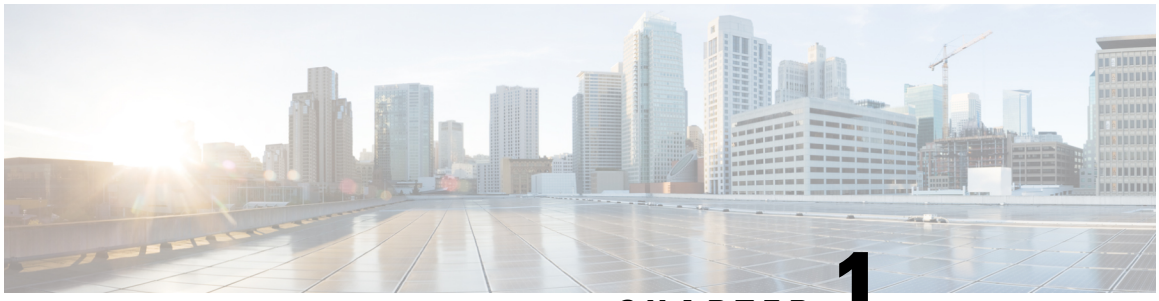
Cisco Secure Firewall Management Center Terminal Services Agent Guide, Version 1.3

First Published: 2021-03-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Introduction to the Management Center Terminal Services Agent

About the Management Center Terminal Services Agent

The Secure Firewall Management Center terminal services agent allows the Secure Firewall Management Center (formerly 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 management center 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 management center 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 management center. 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 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 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.

System Requirements

This version of the TS agent supports connecting to standalone or high availability management centers running Version 6.4 or later of the System.

Troubleshooting Management Center Issues with the TS Agent

See the following sections for information about troubleshooting management center issues with the TS agent.

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

Management Center 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 management center 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 management center.

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.

TS Agent port translation is not performed as expected

If you manually edit the IP address of the server, you must edit the **Server NIC** on the TS agent. Then, save your TS agent configuration and reboot your server.

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.

User sessions are not reported to the Management Center as expected

If you update the TS agent configuration to connect to a different management center, you must end all current user sessions before saving the new configuration. For more information, see Ending a Current User Session, on page 23.

Client application traffic is reported to the Management Center 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-Management Center 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-Management Center connection failure occurs if an incorrectly closed port falls within the **System Ports** range.

TS Agent-Management Center connection failure

If the TS agent fails to establish a connection with the management center 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 management center at the same time.
- Confirm that the **Username** and **Password** you provided are the correct credentials for a management center user with REST VDI privileges as discussed in Creating the REST VDI Role, on page 17.

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

  If the secondary is the active management center, the connection to the primary management center 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.

Management Center shows Unknown users from the TS Agent

The management center 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 management center.
- 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 management center sees the users as Unknown. To resolve the issue, disable web traffic proxying.
- If the primary management center 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 management center and the TS agent reports user session data, the data is logged as Unknown user activity on the management center.
- If the user was previously seen on the management center, 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

Management Center 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 management center 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, on page 13.
- 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 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.

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*.

Resolved Issues

Resolved Issues

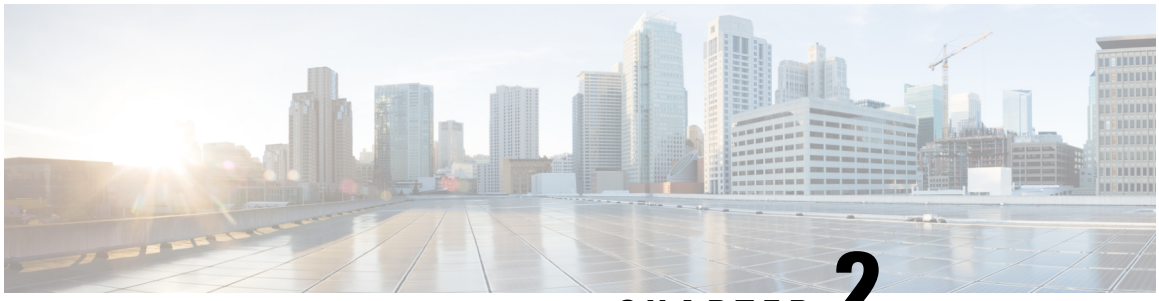
Caveat ID Number	Description
CSCvp10012	Windows Server no longer becomes unresponsive if TS agent is installed.

Caveat ID Number	Description
CSCvn28482	TS Agent no longer becomes unresponsive when performing a TAC dump. In addition, an XML file with driver filters was added to the dump.

History for TS Agent

Feature	Version
• Added support for Citrix Provisioning • The value you specify in the TS agent **Reserve Port(s)** field must match one of the 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
• Detects an IP address change on the server, prompts you to save configuration and reboot. See TS Agent Configuration Fields, on page 13. • Enables you to upgrade to this version without uninstalling the previous version. See Install or Upgrade the TS Agent, on page 11. • Renamed **Exclude Port(s)** configuration field to **Reserve Port(s)**. See TS Agent Configuration Fields, on page 13. • Support for ephemeral ports. See TS Agent Configuration Fields, on page 13. • 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, on page 19. • User session port ranges assigned on least recently used basis. See About the Management Center Terminal Services Agent, on page 1. • Enables you to export troubleshooting information to an XML file. See View Information About the TS Agent, on page 19. • Enables you to restream user sessions to the management center. See View Information About the TS Agent, on page 19. • Attempts to end all user sessions when TS agent is uninstalled. See Uninstalling the TS Agent, on page 24.	1.2

Feature	Version
• 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, on page 13.	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



CHAPTER 2

Install and Configure the TS Agent

Install or Upgrade the TS Agent

Before you begin

- Confirm that the TS agent is supported in your environment, as described in Server and System Environment Requirements, on page 2.
- End all current user sessions as described in Ending a Current User Session, on page 23.

Step 1 Log in to your server as a user with Administrator privileges.

Step 2 Download the TS agent package from the Support site: `TSAgent-1.3.0.exe`.

Note Download the update directly from the site. If you transfer the file by email, it might become corrupted.

Step 3 Right-click `TSAgent-1.3.0.exe` and choose **Run as Administrator**.

Step 4 Click **Install** and follow the prompts to install or upgrade the TS agent.
You are required to reboot the computer before you can use the TS agent.

What to do next

- Confirm the TS agent is running as discussed in Viewing the Status of the TS Agent Service Component, on page 23.
- Start the TS agent as discussed in Starting and Stopping the TS Agent Processes, on page 24.
- Configure the TS agent as discussed in Configure the TS Agent, on page 12.

  If you're upgrading from an earlier TS agent version, and you're using Citrix Provisioning, you must enter **`6910`** in the **Reserve Port(s)** field after you upgrade.

Note If the TS agent installer reports that the .NET Framework failed, run Windows Update and try installing the TS agent again.

Start the TS Agent Configuration Interface

cite

If there is a TS agent shortcut on your desktop, double-click on the shortcut. Otherwise, use the following procedure to launch the TS agent configuration interface.

Step 1 Log in to your server as a user with Administrator privileges.

Step 2 Open `C:\Program Files (x86)\Cisco\Terminal Services Agent`.

Step 3 View the program files for the TS agent.

Note The program files are view-only. Do not delete, move, or modify these files.

Step 4 Double-click the `TSAgentApp` file to start the TS agent.

Configure the TS Agent

Use the TS agent interface to configure the TS agent. You must save your changes and reboot the server for your changes to take effect.

Before you begin

- If you are connecting to the System, configure and enable one or more Active Directory realms targeting the users your server is monitoring, as described in the *Cisco Secure Firewall Management Center Configuration Guide*.
- If you are connecting to the System, configure a user account with REST VDI privileges.

  You must create the REST VDI role in the management center as discussed in Creating the REST VDI Role, on page 17.
- If you are already connected to the System and you are updating your TS agent configuration to connect to a different management center, you must end all current user sessions before saving the new configuration. For more information, see Ending a Current User Session, on page 23 .
- Synchronize the time on your TS agent server with the time on your System.
- Review and understand the configuration fields, as described in TS Agent Configuration Fields, on page 13.

Step 1 On the server where you installed the TS agent, start the TS agent as described in Start the TS Agent Configuration Interface, on page 12.

Step 2 Click **Configure**.

Step 3 Navigate to the General settings section of the tab page.

Step 4 Enter a **Max User Sessions** value.

Step 5 Choose the **Server NIC** to use for port translation and communications.

If the server's IP address changes later, you are prompted to save the configuration and reboot the server to make the change effective.

Step 6 Enter **System Ports** and **User Ports** values. In a valid configuration, the system and user port ranges do not overlap.

Step 7 Enter **Reserve Port(s)** values as a comma-separated list.

Reserve Port(s) is automatically populated with expected values for the Citrix MA Client (2598), Citrix Provisioning (6910), and Windows Terminal Server (3389) ports. You must exclude the Citrix MA Client and Windows Terminal Server ports.

If you're using Citrix Provisioning and you're upgrading from an earlier TS agent version, you must enter `6910` in this field.

Step 8 Navigate to the REST API Connection settings section of the tab.

Step 9 Enter **Hostname/IP Address** and **Port** values.

The management center requires **Port** 443.

Step 10 Enter the **Username** and **Password**.

Step 11 Optionally, repeat steps 9 and 10 in the second row of fields to configure a standby (failover) connection.

Step 12 Click **Test** to test the REST API connection between the TS agent and the system.

If you have a primary and secondary management center configured, the test connection to the secondary fails. This is expected behavior. The TS agent communicates with the active management center at all times. If the primary fails over and becomes the inactive management center, the TS agent communicates with the secondary (now active) management center.

Step 13 Click **Save** and confirm that you want to reboot the server.

TS Agent Configuration Fields

The following fields are used to configure the settings on a TS agent.

General Settings

Table 1: General Settings Fields

Field	Description
Reserve Port(s)	The port(s) you want the TS agent to ignore. Enter the ports you want to exclude comma-separated list. The TS agent automatically populates **Reserve Port(s)** with default port values f MA Client (2598), Citrix Provisioning (6910), and Windows Terminal Server (3 do not exclude the proper ports, applications requiring those ports might fail. The value you specify in the TS agent **Reserve Port(s)** field must match one of t Provisioning **First and Last UDP port numbers** ports. **Caution** Failure to specify the correct port will cause clients to fail to boot. **Note** If a process on your server is using or listening in on a port that is n **System Ports** range, you must manually exclude that port using the **Port(s)** field. **Note** If there is a client application installed on your server and the applic configured to bind to a socket using a specific port number, you mu **Reserve Port(s)** field to exclude that port from translation.
Max User Sessions	The maximum number of user sessions you want the TS agent to monitor. A sing run several user sessions at a time. This version of the TS agent supports 29 user sessions by default, up to a maxim user sessions.
Server NIC	This version of the TS agent supports using a single network interface controller (translation and server-system communications. If two or more valid NICs are pr server, the TS agent performs port translation only on the address you specify du configuration. The TS agent automatically populates this field with the IPv4 address and/or IPv each NIC on the server where the TS agent is installed. A valid NIC must have a or IPv6 address, or one of each type; a valid NIC cannot have multiple addresses type. **Note** If the server's IP address changes, you are prompted to save the confi reboot the server to make the change effective. **Note** You must disable router advertisement messages on any devices con your server. If router advertisements are enabled, the devices may ass IPv6 addresses to NICs on your server and invalidate the NICs for u TS agent.

Field	Description
System Ports	The port range you use for system processes. The TS agent ignores this activ **Start** port to indicate where you want to begin the range. Configure a **Range** the number of ports you want to designate for each individual system proces Cisco recommends a **Range** value of 5000 or more. If you notice the TS agen out of ports for system processes, increase your **Range** value. **Note** If a system process requires a port that falls outside your designate add the port to the **Exclude Port(s)** field. If you do not identify system processes in the **System Ports** range or exclude it, system fail. The TS agent automatically populates the **End** value using the following for `( [Start value] + [Range value] ) - 1` If your entries cause the **End** value to exceed the **Start** value of **User Ports**, your **Start** and **Range** values.
User Ports	The port range you want to designate for users. Configure a **Start** port to ind want to begin the range. Configure a **Range** value to indicate the number of p designate for TCP or UDP connections in each individual user session. **Note** ICMP traffic is passed without being port mapped. Cisco recommends a **Range** value of 1000 or more. If you notice the TS agen out of ports for user traffic, increase your **Range** value. **Note** When the number of ports used exceeds the value of **Range**, user t The TS agent automatically populates the **End** value using the following for `[Start value] + ( [Range value] * [Max User Sessions value] ) -` If your entries cause the **End** value to exceed 65535, you must adjust your **S** values.
Ephemeral Ports	Enter a range of ephemeral ports (also referred to as *dynamic ports*) to allow monitor.

Field	Description
Unknown Traffic Communication	Check **Permit** to allow the TS agent to permit traffic over System ports; however, does not track port usage. System ports are used by the Local System account or user accounts. (A local user account exists only on the TS agent server; it has no c Active Directory account.) You can choose this option to permit the following ty • Permit traffic run by the Local System account (such as Server Message Bl instead of being blocked. The management center identifies this traffic as c the Unknown user because the user does not exist in Active Directory. Enabling this option also enables you to successfully test the connection wi management center if you log in to the TS agent server using a local system • When a user or system session exhausts all available ports in its range, the TS the traffic over ephemeral ports. This option enables the traffic; the manage identifies the traffic as coming from the Unknown user. This is especially useful when System ports are needed for keeping system as domain controller updates, authentications, Windows Management Inter queries, and so on. Uncheck to block traffic on system ports.

REST API Connection Settings

You can configure a connection primary and, optionally, standby (failover) system appliances:

- If your system appliance is standalone, leave the second row of REST API Connection fields blank.
- If your system appliance is deployed with a standby (failover) appliance, use the first row to configure a connection to the primary appliance and the second row to configure a connection to the standby (failover) appliance.

Table 2: REST API Connection Settings Fields

Field	Description
Hostname/IP Address	The hostname or IP address for the system appliance.
Port	The port the system uses for REST API communications. (The management cen uses port 443.)
Username and Password	The credentials for the connection. • The System requires a username and password for a user with REST VDI p the management center. For more information about configuring this user, s *Secure Firewall Management Center Configuration Guide*.

Creating the REST VDI Role

To connect the TS agent to the management center, your user must have the REST VDI role. The REST VDI is not defined by default. You must create the role and assign it to any user that is used in the TS agent configuration.

For more information about users and roles, see the *Cisco Secure Firewall Management Center Configuration Guide*.

Step 1 Log in to the management center as a user with permissions to create roles.

Step 2 Click **System** > **Users**.

Step 3 Click the **User Roles** tab.

Step 4 On the User Roles tab page, click **Create User Role**.

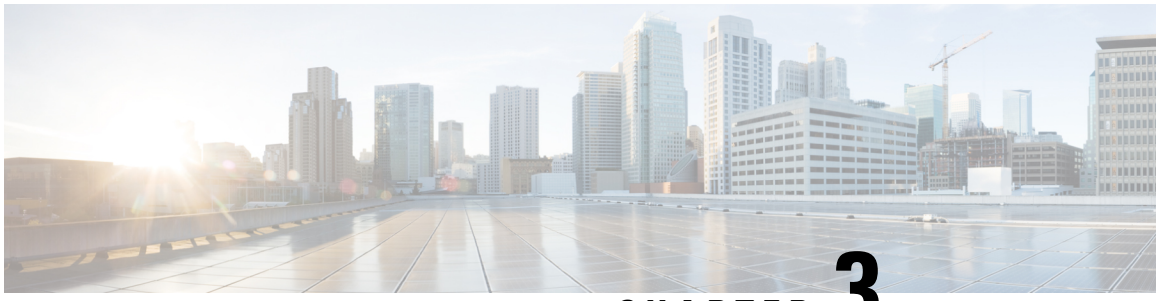
Step 5 In the Name field, enter `REST VDI`.

The role name is not case-sensitive.

Step 6 In the Menu-Based Permissions section, check **REST VDI** and make sure **Modify REST VDI** is also checked.

Step 7 Click **Save**.

Step 8 Assign the role to the user that is used in the TS agent configuration.



CHAPTER 3

View TS Agent Data

View Information About the TS Agent

Use the following procedure to view the current user sessions on the network and the port ranges assigned to each session. The data is read-only.

Step 1 On the server where you installed the TS agent, start the TS agent interface as described in Start the TS Agent Configuration Interface, on page 12.

Step 2 Click the **Monitor** tab. The following columns are displayed:

- **REST Server ID**: Host name or IP address of the management center that is reporting the information. This information is useful if you have a high availability configuration.
- **Source IP**: Displays the user's IP address value in IPv4 and/or IPv6 format. When both IPv4 and IPv6 addresses are configured and a new session is just created, both IPv4 and IPv6 addresses are displayed in separate rows.
- **Status**: Displays the status of assigning ports to the user. For more information, see View Connection Status, on page 20.
- **Session ID**: Number that identifies the user's session. A user can have more than one session at a time.
- **Username**: Username associated with the session.
- **Domain**: Active Directory domain in which the user logged in.
- **Port Range**: Port range assigned to the user. (A value of `0` indicates an issue assigning ports; for more information, see View Connection Status, on page 20).
- **TCP Ports Usage** and **UDP Ports Usage**: Displays the percentage of allocated ports per user. When the percentage exceeds 50%, the field background is yellow. When the percentage exceeds 80%, the field background is red.
- **Login Date**: Date the user logged in.

Step 3 The following table shows the actions you can perform:

Item	Description
Click column heading	Sort data in the table by that column.

Item	Description
	Enter a portion of a username or a complete username in the **Filter by Username** search field.
	Click to refresh sessions displayed on this tab page.
	Export the following troubleshooting information about the TS agent as text files: • XML file containing TS agent configuration data • Output from the **netstat -a -n -o** command • Windows task list • List of running drivers
	Check the box next to one or more session to restream those sessions to the management center. You can use this in the event the user service fails on the management center. For example, suppose a user logs in to the TS agent server after the user service fails on the management center. You can use this option to send the user session again after the user service is restored. This should cause **Success** to be displayed for that user in the Status column.

View Connection Status

When users have logged into Terminal Services where TS agent is installed, a new system session is created, a port range is allocated for this session, and the results are sent to management center for propagation to managed devices.

The Monitor tab page enables you to confirm that the port range was successfully sent to the management center. Among the reasons why the process might have failed include:

- Network connectivity issues

  Invalid VDI credentials
- Token expiration
- Incorrect domain name configured for the realm

Step 1 On the server where you installed the TS agent, start the TS agent interface as described in Start the TS Agent Configuration Interface, on page 12.

Step 2 Click the **Monitor** tab.

Step 3 The Status column has one of the following values:

- **Pending**: The action is pending but not yet completed.

- **Failed**: The action failed. Click the word **Failed** to view an error message. If the error indicates a communication failure with the management center, try to restream traffic for that session as discussed in View Information About the TS Agent.
- **Success**: The action completed successfully.

View TS Agent User, User Session, and TCP/UDP Connection Data on the Management Center

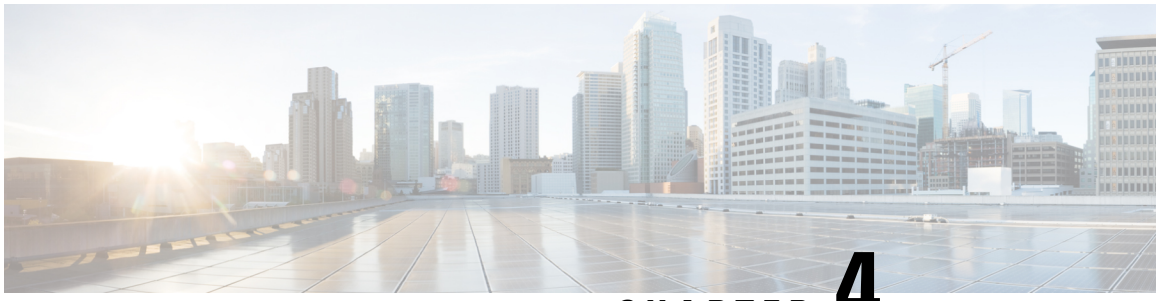
Use the following procedure to view data reported by the TS agent. For more information about the management center tables, see the *Cisco Secure Firewall Management Center Configuration Guide*.

Step 1 Log in to the management center where you configured the realms targeting the users your server is monitoring.

Step 2 To view users in the Users table, choose **Analysis** > **Users** > **Users**. The management center populates the **Current IP**, **End Port**, and **Start Port** columns if a TS agent user's session is currently active.

Step 3 To view user sessions in the User Activity table, choose **Analysis** > **Users** > **User Activity**. The management center populates the **Current IP**, **End Port**, and **Start Port** columns if the TS agent reported the user session.

Step 4 To view TCP/UDP connections in the Connection Events table, choose **Analysis** > **Connections** > **Events**. The management center populates the **Initiator/Responder IP** field with the IP address of the TS agent that reported the connection and the **Source Port/ICMP Type** field with the port the TS agent assigned to the connection.



CHAPTER 4

Manage the TS Agent

Ending a Current User Session

Use the following procedure to log off a user from the network and end their session.

Step 1 Log in to your TS agent server as a user with administrator privileges.

Step 2 Open **Start** > **> [All Programs]** > **Task Manager**.

Step 3 Expand the window by clicking **More Details**.

Step 4 Click the **Users** tab.

Step 5 (Optional) To notify a user that you are ending their session, right-click on the user session and choose **Send message**.

Step 6 Right-click on the user session and choose **Sign off**.

Step 7 Click **Sign out user** to confirm the action.

Viewing the Status of the TS Agent Service Component

Use the following procedure to confirm that the TS agent service component is running. For more information about the service component, see About the Management Center Terminal Services Agent, on page 1.

Step 1 Log in to your server as a user with administrator privileges.

Step 2 Open **Start** > **Tools** > **Services**.

Step 3 Locate `CiscoTSAgent` and view the **Status**.

Step 4 (Optional) If the TS agent service component is stopped, start the TS agent service as described in Starting and Stopping the TS Agent Processes, on page 24.

Starting and Stopping the TS Agent Processes

Use the following procedure to start or stop the TS agent service component.

Step 1 Log in to your server as a user with administrator privileges.

Step 2 Open **Start** > **Administrative Tools** > **Services**.

Step 3 Navigate to the `CiscoTSAgent` and right-click to access the context menu.

Step 4 Choose **Start** or **Stop** to start or stop the TS agent Service.

Viewing TS Agent Activity Logs on the Server

If prompted by Support, use the following procedure to view the activity logs for the service component.

Open **Tools** > **Event Viewer** > **Applications and Services Log** > **Terminal Services Agent Log**.

Uninstalling the TS Agent

Use the following procedure to uninstall the TS agent from your server. Uninstalling the TS agent removes the interface, service, and driver from your server. Uninstalling the TS agent also terminates active user sessions as reported to the management center. The strong cryptography modification is not removed.

Step 1 Log in to your server as a user with administrator privileges.

Step 2 Open **Start** > **Control Panel**.

Step 3 Click **All Control Panel Items** > **Programs and Features**.

Step 4 Right-click **Terminal Services Agent** and choose **Uninstall**.