



Cisco Terminal Services (TS) Agent Guide, Version 1.0

First Published: 2016-08-29

Last Modified: 2018-01-30

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Introduction to the Terminal Services (TS) Agent	1
	About the Cisco Terminal Services (TS) Agent	1
	Server and System Environment Requirements	2
	Troubleshooting Firepower Management Center Issues with the TS Agent	3
	Troubleshoot Issues with the TS Agent	6
	Troubleshoot Issues with the User Agent	6
	Known Issues and Resolved Issues	7
	History for TS Agent	8

CHAPTER 2	Install and Configure the TS Agent	9
	Install the TS Agent	9
	Start the TS Agent Configuration Interface	10
	Configure the TS Agent	10
	TS Agent Configuration Fields	11
	Creating the REST VDI Role	16

CHAPTER 3	View TS Agent Data	17
	View Information About the TS Agent	17
	View TS Agent User, User Session, and TCP/UDP Connection Data on the Firepower Management Center	18

CHAPTER 4	Manage the TS Agent	19
	Ending a Current User Session	19
	Viewing the Status of the TS Agent Service Component	19
	Starting and Stopping the TS Agent Processes	20
	Viewing TS Agent Activity Logs on the Server	20

Uninstalling the TS Agent 20



CHAPTER

1

Introduction to the Terminal Services (TS) Agent

- [About the Cisco Terminal Services \(TS\) Agent, on page 1](#)
- [Server and System Environment Requirements, on page 2](#)
- [Troubleshooting Firepower Management Center Issues with the TS Agent, on page 3](#)
- [Troubleshoot Issues with the TS Agent, on page 6](#)
- [Troubleshoot Issues with the User Agent, on page 6](#)
- [Known Issues and Resolved Issues, on page 7](#)
- [History for TS Agent, on page 8](#)

About the Cisco 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](#). You can't upgrade the TS Agent; you must uninstall the older version before you install the newer version. For more information, see [Uninstalling the TS Agent, on page 20](#).

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.



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 installation also modifies your server's Microsoft .NET Framework to use strong cryptography (TLS 1.2) for all communications. View the "SchUseStrongCrypto"=dword:00000001 modification in your Windows Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\.

The TS Agent can be used for the following:

- TS Agent data on the Firepower Management Center 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*.

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](#). You can't upgrade the TS Agent; you must uninstall the older version before you install the newer version. For more information, see [Uninstalling the TS Agent, on page 20](#).

Server Requirements

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

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2



Note

The TS Agent installation requires 576 KB 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.

Firepower System Requirements

This version of the TS Agent supports connecting to standalone or high availability Firepower Management Centers running Version 6.2 or later of the Firepower 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](#).

Firepower 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 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 Firepower 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 199, the TS Agent does not perform port translation on the 200th user session.
- All available ports are in use. For example, if your **User Ports Range** value designates 200 ports per user session, the TS Agent does not perform port translation on the 201st 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.

User sessions are not reported to the Firepower Management Center as expected

If you update the TS Agent configuration to connect to a different Firepower 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 19](#).

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

TS Agent-Firepower Management Center connection failure

If the TS Agent fails to establish a connection with the Firepower 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 FMC at the same time.
- Confirm that the **Username** and **Password** you provided are the correct credentials for a Firepower Management Center user with REST VDI privileges as discussed in [Creating the REST VDI Role, on page 16](#).

You can view the audit logs on the Firepower Management Center to confirm that the user authentication from the TS Agent succeeded.

- If the connection to the secondary Firepower Management Center in a high availability configuration fails immediately after configuration, this is expected behavior. The TS Agent communicates with the active Firepower Management Center at all times.

If the secondary is the active Firepower Management Center, the connection to the primary Firepower 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.

Firepower Management Center shows Unknown users from the TS Agent

The Firepower 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 Firepower 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 FMC sees the users as Unknown. To resolve the issue, disable web traffic proxying.
-
- If the primary Firepower 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 Firepower Management Center and the TS Agent reports user session data, the data is logged as Unknown user activity on the Firepower Management Center.
 - If the user was previously seen on the Firepower 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

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
CSCve54339	<p>UDP traffic is getting blocked, especially if the port is allocated in the operating system's ephemeral range (ports 49152 to 65535).</p> <p>Workaround: Either reboot the server or uninstall the TS Agent.</p>
CSCve49682	<p>The TS Agent drops listening ports before they are unbound.</p> <p>If hosts where TS Agent is installed have services or applications listening on ports to receive connections from clients, the TS Agent updates its tables of such ports to allocate (when implicit bound is requested) a port, or allow when it is an explicit bind.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> • For cases where the listening ports are well-known, the ports can be added to the Exclude Port(s) list. • For Windows Management Instrumentation (WMI) specifically, a fixed range or a single port can be configured and then you can exclude those ports. • For any other case where ports are randomly bound and there is no previous knowledge of those ports, there is no workaround.
CSCvf25546	<p>Fewer ports are available for connections when both IPv4 and IPv6 are configured on the monitored network adapter.</p>
CSCvf63615	<p>At debug level 6, some incorrect function names display in the logs.</p>
CSCvf65188	<p>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:</p> <pre>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.</pre> <p>Workarounds:</p> <ul style="list-style-type: none"> • Increase the number of ports in the range. • Decrease the time TCP stack has to wait until such connections are fully released: <code>TcpTimedWaitDelay</code>, found in the following location in the Windows registry: <code>HKEY_LOCAL-MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters</code> For more information, see the description of <code>TcpTimedWaitDelay</code> on MSDN.

Caveat ID Number	Description
CSCvg65253	User IP bindings are not being sent to the Firepower Management Center, and both TS Agent event viewer log and the Status column on the TS Agent's Monitor tab page show: FMC_STATS_TO_BE_CONNECT. Workaround: Wait until system has completed rebooting and is stable, then restart the TS Agent service. Data should then be reported to the Firepower Management Center.

Resolved Issues

Caveat ID Number	Description
CSCve09114	Removed Firepower Management Center and FMC wording from on-screen messages.
CSCve09083	The TS Agent installer now depends on the latest available .NET Framework, which at the time of this writing is 4.6.2. This is required to support TLS 1.2. Unlike previous TS Agent versions, no registry entry is created.
CSCve09055	The REST API Connection host name is accepted by the TS Agent, even if the host name contains capital letters or multiple tokens such as <code>this.is.a.domain.example</code> .
CSCvd79876	The TS Agent's REST request no longer tracks whether or not the token is expired.

History for TS Agent

Feature	Version
<p>TS Agent</p> <p>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.</p>	1.0



CHAPTER 2

Install and Configure the TS Agent

- [Install the TS Agent, on page 9](#)
- [Start the TS Agent Configuration Interface, on page 10](#)
- [Configure the TS Agent, on page 10](#)
- [Creating the REST VDI Role, on page 16](#)

Install 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](#).
- If you previously installed the TS Agent, uninstall the TS Agent as described in [Uninstalling the TS Agent, on page 20](#).
- End all current user sessions as described in [Ending a Current User Session, on page 19](#).

Procedure

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-1.0.0-36.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-1.0.0-36.exe](#) and choose **Run as Administrator**.

Step 4 Click **Install** and follow the prompts to install 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 19](#).

- Start the TS Agent as discussed in [Starting and Stopping the TS Agent Processes, on page 20](#).
- Configure the TS Agent as discussed in [Configure the TS Agent, on page 10](#).



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.

Procedure

- 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 Firepower System, configure and enable one or more Active Directory realms targeting the users your server is monitoring, as described in the *Firepower Management Center Configuration Guide*.
- If you are connecting to the Firepower System, configure a user account with REST VDI privileges. You must create the REST VDI role in the Firepower Management Center as discussed in [Creating the REST VDI Role, on page 16](#).
- If you are already connected to the Firepower System and you are updating your TS Agent configuration to connect to a different Firepower 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 19](#).
- Synchronize the time on your TS Agent server with the time on your Firepower System.

- Review and understand the configuration fields, as described in [TS Agent Configuration Fields, on page 11](#).

Procedure

- 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 10](#).
- 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.
- 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 **Exclude Port(s)** values as a comma-separated list.
- Exclude Port(s)** is automatically populated with expected values for the Citrix MA Client (2598), and Windows Terminal Server (3389) ports. You must exclude the Citrix MA Client and Windows Terminal Server ports.
- Step 8** Navigate to the Firepower Management Center settings section of the tab.
- Step 9** Enter **Host** and **Port** values.
- The Firepower 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 Firepower Management Center configured, the test connection to the secondary fails. This is expected behavior. The TS Agent communicates with the active Firepower Management Center at all times. If the primary fails over and becomes the inactive Firepower Management Center, the TS Agent communicates with the secondary (now active) Firepower 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	Example
Exclude Port(s)	<p>The port(s) you want the TS Agent to ignore. Enter the ports you want to exclude as a comma-separated list.</p> <p>The TS Agent automatically populates Exclude Port(s) with default port values for the Citrix MA Client (2598), and Windows Terminal Server (3389). If you do not exclude the proper ports, applications requiring those ports might fail.</p> <p>Note If a process on your server is using or listening in on a port that is not in your System Ports range, you must manually exclude that port using the Exclude Port(s) field.</p> <p>Note If there is a client application installed on your server and the application is configured to bind to a socket using a specific port number, you must use the Exclude Port(s) field to exclude that port from translation.</p>	<p>Typically one of the following:</p> <ul style="list-style-type: none"> 2598, 3389 (the Citrix MA Client and Windows Terminal Server ports)
Max User Sessions	<p>The maximum number of user sessions you want the TS Agent to monitor. A single user can run several user sessions at a time.</p> <p>This version of the TS Agent supports up to 199 user sessions.</p>	199 (the maximum supported value in this version of the TS Agent)

Field	Description	Example
Server NIC	<p>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.</p> <p>The TS Agent automatically populates this field with the IPv4 address and/or IPv6 address for each NIC on the server where the TS Agent is installed. 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.</p> <p>Note 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.</p> <p>Note You must disable router advertisement messages on any devices connected to your server. If router advertisements are enabled, the devices may assign multiple IPv6 addresses to NICs on your server and invalidate the NICs for use with the TS Agent.</p>	Ethernet 2 (192.0.2.1) (a NIC on your server)

Field	Description	Example
System Ports	<p>The port range you use for system processes. The TS Agent ignores this activity. Configure a Start port to indicate where you want to begin the range. Configure a Range value to indicate the number of ports you want to designate for each individual system process.</p> <p>Cisco recommends a Range value of 200 or more. If you notice the TS Agent frequently runs out of ports for system processes, increase your Range value.</p> <p>Note If a system process requires a port that falls outside your designated System Ports, add the port to the Exclude Port(s) field. If you do not identify a port used by system processes in the System Ports range or exclude it, system processes might fail.</p> <p>The TS Agent automatically populates the End value using the following formula:</p> $([Start\ value] + [Range\ value]) - 1$ <p>If your entries cause the End value to exceed the Start value of User Ports, you must adjust your Start and Range values.</p>	<p>Start set to 1024 and Range set to 1000</p>

Field	Description	Example
User Ports	<p>The port range you want to designate for users. Configure a Start port to indicate where you want to begin the range. Configure a Range value to indicate the number of ports you want to designate for TCP or UDP connections in each individual user session.</p> <p>Note ICMP traffic is passed without being port mapped.</p> <p>Cisco recommends a Range value of 200 or more. If you notice the TS Agent frequently runs out of ports for user traffic, increase your Range value.</p> <p>Note When the number of ports used exceeds the value of Range, user traffic is blocked.</p> <p>The TS Agent automatically populates the End value using the following formula:</p> $[\text{Start value}] + ([\text{Range value}] * [\text{Max User Sessions value}]) - 1$ <p>If your entries cause the End value to exceed 65535, you must adjust your Start and Range values.</p>	<p>Start set to 2024 and Range set to 200</p>

Firepower Management Center Settings

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

- If your system appliance is standalone, leave the second row of Firepower Management Center 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: Firepower Management Center Settings Fields

Field	Description	Example
Hostname / IP Address	The hostname or IP address for the primary Firepower Management Center.	192 . 0 . 2 . 1
Port	The port the Firepower Management Center uses for REST API communications. The TS Agent automatically populates this field to 443 , the REST API port on the Firepower Management Center.	443
Username and Password	The Firepower System username and password for a user with REST VDI privileges on the Firepower Management Center. For more information about configuring this user, see Creating the REST VDI Role, on page 16 .	n/a

Creating the REST VDI Role

To connect the TS Agent to the Firepower Management Center, your Firepower 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 *Firepower Management Center Configuration Guide*.

Procedure

-
- Step 1** Log in to the Firepower 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, on page 17](#)
- [View TS Agent User, User Session, and TCP/UDP Connection Data on the Firepower Management Center, on page 18](#)

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.

Procedure

- 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 10](#).
- Step 2** Click the **Monitor** tab. The following columns are displayed:
- **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.
 - **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.
	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.

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

Use the following procedure to view data reported by the TS Agent. For more information about the Firepower Management Center tables, see the *Firepower Management Center Configuration Guide*.

Procedure

- Step 1** Log in to the Firepower 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 Firepower 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 Firepower 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 Firepower 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, on page 19](#)
- [Viewing the Status of the TS Agent Service Component, on page 19](#)
- [Starting and Stopping the TS Agent Processes, on page 20](#)
- [Viewing TS Agent Activity Logs on the Server, on page 20](#)
- [Uninstalling the TS Agent, on page 20](#)

Ending a Current User Session

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

Procedure

- 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 Cisco Terminal Services \(TS\) Agent, on page 1](#).

Procedure

- 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 20](#).
-

Starting and Stopping the TS Agent Processes

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

Procedure

- 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.

Procedure

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. The strong cryptography modification is not removed.

Before you begin

- End all current user sessions as described in [Ending a Current User Session, on page 19](#).

Procedure

- 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**.
