



Cisco Terminal Services (TS) Agent Guide, Version 1.4

First Published: 2022-01-19

Last Modified: 2022-10-14

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



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
	Troubleshoot On-Prem Firewall Management CenterFMCIssues with the TS Agent	3
	Resolved Issues	5
	History for TS Agent	5

CHAPTER 2	Install and Configure the TS Agent	7
	Install or Upgrade the TS Agent	7
	Start the TS Agent Configuration Interface	8
	Set up a Proxy	8
	Set Up an Application Proxy	8
	Get an API Token	9
	Configure the TS Agent	10
	TS Agent Configuration Fields	11
	Creating the REST VDI Role	15

CHAPTER 3	View TS Agent Data	17
	View Information About the TS Agent	17
	View Connection Status	18
	View TS Agent User, User Session, and TCP/UDP Connection Data on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC	19

CHAPTER 4	Manage the TS Agent	21
	Ending a Current User Session	21

Viewing the Status of the TS Agent Service Component	21
Starting and Stopping the TS Agent Processes	22
Viewing TS Agent Activity Logs on the Server	22
Uninstalling the TS Agent	22

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)

© 2019 Cisco Systems, Inc. All rights reserved.



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](#)
- [Troubleshoot On-Prem Firewall Management CenterFMCIssues with the TS Agent, on page 3](#)
- [Resolved Issues, on page 5](#)
- [History for TS Agent, on page 5](#)

About the Cisco Terminal Services (TS) Agent

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

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

- The Cloud-delivered Firewall Management Center available with the Cisco Defense Orchestrator (CDO).
- The On-Prem Firewall Management CenterFMC available with CDO.
- A standalone Management Center or high availability system that is not associated with CDO.

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



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

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



Note ICMP messages are passed without port mapping.

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

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

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

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

- Interface—application to configure the TS Agent and monitor the current user sessions
- Service— program that monitors the user logins and logoffs
- Driver— program that performs the port translation

The TS Agent can be used for the following:

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



Note To use TS Agent for user awareness and control, you must configure it to send data *only* to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. For more information, see [Configure the TS Agent, on page 10](#).

Server and System Environment Requirements

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



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

Server Requirements

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

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012

- Microsoft Windows Server 2012 R2

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

- Microsoft .NET Framework 4.6.2
- Microsoft Visual C++ Update 4



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



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

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

- Citrix Provisioning
- Citrix XenDesktop
- Citrix XenApp
- Xen Project Hypervisor
- VMware vSphere Hypervisor/VMware ESXi 6.0
- Windows Terminal Services/Windows Remote Desktop Services (RDS)

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



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

Troubleshoot On-Prem Firewall Management CenterFMC Issues with the TS Agent

On-Prem Firewall Management CenterFMC test connection fails

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

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 11](#).
- 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 Provisioning clients fail to boot

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

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



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

Exceptions when saving the TS Agent IP address

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

- The same IP address as another device on the network.
- Changing the static IP address in Windows while the TS Agent application is open.

Exceptions include the following:

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

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

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

Resolved Issues

Resolved Issues

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

History for TS Agent

Feature	Version
Supports both the On-Prem Firewall Management Center FMC and Cloud-delivered Firewall Management Center available with the Cisco Defense Orchestrator, as well as a standalone Management Center.	1.4
<ul style="list-style-type: none"> • Added support for Citrix Provisioning • The value you specify in the TS Agent Reserve Port(s) field must match one of the Citrix Provisioning First and Last UDP port numbers ports. <p>Caution Failure to specify the correct port will cause clients to fail to boot.</p>	1.3

Feature	Version
<ul style="list-style-type: none"> • Detects an IP address change on the server, prompts you to save configuration and reboot. See TS Agent Configuration Fields, on page 11. • Enables you to upgrade to this version without uninstalling the previous version. See Install or Upgrade the TS Agent, on page 7. • Renamed Exclude Port(s) configuration field to Reserve Port(s). See TS Agent Configuration Fields, on page 11. • Support for ephemeral ports. See TS Agent Configuration Fields, on page 11. • 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 17. • User session port ranges assigned on least recently used basis. See About the Cisco Terminal Services (TS) Agent, on page 1. • Enables you to export troubleshooting information to an XML file. See View Information About the TS Agent, on page 17. • Enables you to restream user sessions to the Management Center. See View Information About the TS Agent, on page 17. • Attempts to end all user sessions when TS Agent is uninstalled. See Uninstalling the TS Agent, on page 22. 	1.2
<ul style="list-style-type: none"> • Default maximum number of max user sessions changed from 200 to 30. • Port range changed from 200 or more to 5000 or more <p>These changes are all discussed in TS Agent Configuration Fields, on page 11.</p>	1.1
<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 or Upgrade the TS Agent, on page 7](#)
- [Start the TS Agent Configuration Interface, on page 8](#)
- [Set up a Proxy, on page 8](#)
- [Get an API Token, on page 9](#)
- [Configure the TS Agent, on page 10](#)
- [Creating the REST VDI Role, on page 15](#)

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 21](#).

-
- 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-1.4.1.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-1.4.1.exe` and choose **Run as Administrator**.
- Step 4** Click **Install** and follow the prompts to install or upgrade 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 21](#).
- Start the TS Agent as discussed in [Starting and Stopping the TS Agent Processes, on page 22](#).
- Configure the TS Agent as discussed in [Configure the TS Agent, on page 10](#).

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

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.

Set up a Proxy

If your Cloud-Delivered Firewall Management Center cannot communicate with the machine on which TS Agent is installed, you must use a proxy with the HTTPS protocol enabled.

The way you do this is up to you; for example, you might have a commercial proxy and use a Windows system proxy with HTTPS enabled to communicate with it.



Note This task is not required to use an On-Prem Firewall Management Center with the TS Agent or if you are not using CDO at all.

Set Up an Application Proxy

This task provides one suggested option to configure a proxy on the Windows Server on which the TS Agent is running. Cisco provides no assurance this procedure will work in your situation. For more information, consult your proxy provider and [Windows documentation](#).

Before you begin

You must have already set up a proxy server; doing so is beyond the scope of this documentation.

Step 1 Log in as Administrator to your Windows Server.

Step 2 As Administrator, open the following file in a text editor:

```
\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
```

Step 3 Paste the following in `machine.config` in the `<system.net>` section. Replace the sample IP address and port with your proxy server's IP address and port.

```
<!-- Configuration for TS Agent -->
<system.net>
  <defaultProxy>
    <proxy autoDetect="false" bypassonlocal="false" proxyaddress="http://192.0.2.197:3128"
usesystemdefault="false" />
  </defaultProxy>
</system.net>
<!-- Configuration for TS Agent -->
```

Step 4 Save your changes to `machine.config` and exit the text editor.

Step 5 Restart the server for the changes to take effect.

What to do next

See [Get an API Token, on page 9](#).

Get an API Token

This task discusses how to get the API token, which is used by the TS Agent to authenticate with the Cisco Defense Orchestrator.

Required role:

- Super Admin
- Admin
- Deploy Only (or better) with API Only enabled



Note This task applies to Cloud-Delivered Firewall Management Center only.

If you are using On-Prem Firewall Management Center, see [Creating the REST VDI Role, on page 15](#) instead.


Step 1 Log in to CDO as a user with one of the following roles:

- Super Admin: To either create an optional TS Agent user or to get the API token for yourself.
- Admin or Deploy Only with API Only enabled: To get an API token for yourself.

Step 2 (Optional for the Super Admin user only.) Create a user for TS Agent with the Deploy Only or better role and check **API Only**.

Step 3 In the top right corner, click your login name, then click **Settings**.

Step 4 In the General Settings row, click **Generate API Token**.

Step 5 Copy the token to the clipboard; you can click  to do that.

What to do next

Configure the TS Agent as discussed in [Configure the TS Agent, on page 10](#).

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 Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC, 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 Device 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 15](#).
- If you are already connected to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC and you are updating your TS Agent configuration to connect to a different Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC, you must end all current user sessions before saving the new configuration. For more information, see [Ending a Current User Session, on page 21](#).
- Synchronize the time on your TS Agent server with the time on your Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC.
- • Cloud-Delivered Firewall Management Center only:
 - Get an API token as discussed in [Get an API Token, on page 9](#)
- Review and understand the configuration fields, as described in [TS Agent Configuration Fields, on page 11](#).

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 8](#).

Step 2 Click the **Configure** tab.

Step 3 Cloud-Delivered Firewall Management Center only: Click the **Cloud** tab at the bottom of the page.

Step 4 On-Prem Firewall Management Center only: Click the **On-Prem tab** tab at the bottom of the page.

Step 5 See [TS Agent Configuration Fields, on page 11](#).

- Step 6** After you have configured the TS Agent, click **Test** to test the REST API connection between the TS Agent and the system.
- Step 7** 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
Max User Sessions	<p>The maximum number of user sessions you want the TS Agent to monitor. A TS Agent can run several user sessions at a time.</p> <p>This version of the TS Agent supports 29 user sessions by default, up to a maximum of 30 user sessions.</p>
Server NIC	<p>The TS Agent supports using a single network interface controller (NIC) for client-to-agent and server-system communications. If two or more valid NICs are present on the 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 of each NIC on the server where the TS Agent is installed. A valid NIC must have either an IPv4 or IPv6 address, or one of each type; a valid NIC cannot have multiple addresses of the same type.</p> <p>Note If the server's IP address changes, you are prompted to save the configuration and reboot the server to make the change effective.</p> <p>Note You must disable router advertisement messages on any devices connected to your server. If router advertisements are enabled, the devices may send IPv6 addresses to NICs on your server and invalidate the NICs for the TS Agent.</p>

Field	Description
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 5000 or more. If you notice the TS Agent running 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 for system processes in the System Ports range or exclude it, system processes may 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>
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 1000 or more. If you notice the TS Agent running 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 may be dropped.</p> <p>The TS Agent automatically populates the End value using the following formula:</p> $[Start\ value] + ([Range\ value] * [Max\ User\ Sessions\ value]) - 1$ <p>If your entries cause the End value to exceed 65535, you must adjust your Start and Range values.</p>
Ephemeral Ports	<p>Enter a range of ephemeral ports (also referred to as <i>dynamic ports</i>) to allow the TS Agent to monitor.</p>

Field	Description
<p>Unknown Traffic Communication</p>	<p>Check Permit to allow the TS Agent to permit traffic over System ports; how the TS Agent does not track port usage. System ports are used by the Local System account and local user accounts. (A local user account exists only on the TS Agent server and corresponds to a corresponding Active Directory account.) You can choose this option to permit the following types of traffic:</p> <ul style="list-style-type: none"> • Permit traffic run by the Local System account (such as Server Message Block) instead of being blocked. The Cloud-delivered Firewall Management Center (Cloud-Firewall Management Center) or On-Prem Firewall Management Center (On-Prem Firewall Management Center) identifies this traffic as coming from the Unknown user because the user does not exist in Active Directory. <p>Enabling this option also enables you to successfully test the connection to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management Center if you log in to the TS Agent server using a local system account.</p> <ul style="list-style-type: none"> • When a user or system session exhausts all available ports in its range, the TS Agent allows the traffic over ephemeral ports. This option enables the traffic; the Cloud-delivered Firewall Management Center or On-Prem Firewall Management Center identifies the traffic as coming from the Unknown user. <p>This is especially useful when System ports are needed for keeping systems up-to-date, such as domain controller updates, authentications, Windows Management Instrumentation queries, and so on.</p> <p>Uncheck to block traffic on system ports.</p>
<p>Reserve Port(s)</p>	<p>The port(s) you want the TS Agent to ignore. Enter the ports you want to exclude in a comma-separated list.</p> <p>The TS Agent automatically populates Reserve Port(s) with default port values: Citrix MA Client (2598), Citrix Provisioning (6910), and Windows Terminal Services. If you do not exclude the proper ports, applications requiring those ports might fail.</p> <p>If you're using Citrix Provisioning and you're upgrading from an earlier TS Agent version, you must enter 6910 in this field.</p> <p>The value you specify in the TS Agent Reserve Port(s) field must match one of the Citrix Provisioning First and Last UDP port numbers ports.</p> <p>Caution Failure to specify the correct port will cause clients to fail to boot.</p> <p>Note If a process on your server is using or listening in on a port that is in the System Ports range, you must manually exclude that port using the 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 Reserve Port(s) field to exclude that port from translation.</p>

Cloud-delivered Firewall Management Center Settings

Sample **Cloud** tab page:

The screenshot shows the 'Terminal Services Agent' configuration window. The 'Configure' tab is active, and the 'General' section is expanded. The settings are as follows:

- Max User Sessions:** 29
- Server NIC:** Ethernet0 (192.168.0.253)
- System Ports:** Start: 10000, Range: 5000, End: 14999
- User Ports:** Start: 15000, Range: 1000, End: 43999
- Ephemeral Ports:** Start: 49152, Range: 16384, End: 65535
- Unknown Traffic Communication:** Permit
- Reserve Port(s):** 2598,3389,6901

Below the 'General' section, there are tabs for 'On-Prem' and 'Cloud'. The 'Cloud' tab is selected, showing the 'Cloud-Delivered Firewall Management Center REST API' section with fields for Hostname / IP Address, Port, and Token, and a 'Test' button. At the bottom of the window are 'Save' and 'Cancel' buttons.

Table 2: Cloud-delivered Firewall Management Center Settings Fields

Field	Description
Hostname / IP Address	The hostname or IP address of the Cloud-Delivered Firewall Management Center URL that is displayed when you click Tools & Services > Firewall Management Monitoring .
Port	The port the Cloud-Delivered Firewall Management Center uses for REST API communication. The TS Agent automatically populates this field to 443 , the REST API port.
Token	The API token used to authenticate with the Cisco Defense Orchestrator. For more information, see Get an API Token, on page 9 .

On-Prem Firewall Management Center FMC Settings

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

- If your system appliance is standalone, leave the second row of FMC/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.

Sample **On-Prem** tab page:

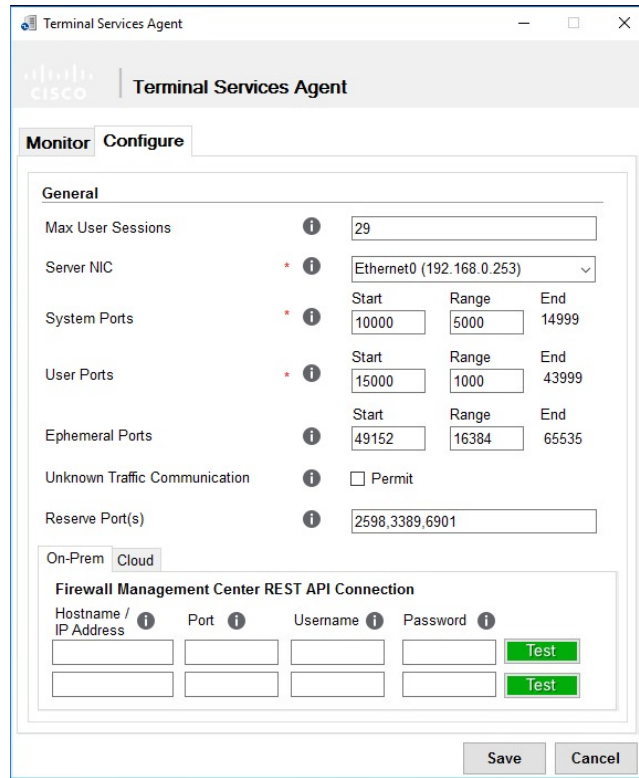


Table 3: or On-Prem Firewall Management CenterFMC Settings Fields

Field	Description
Hostname / IP Address	The hostname or IP address for the primary or On-Prem Firewall Management CenterFMC.
Port	The port the or On-Prem Firewall Management CenterFMC uses for REST VDI communications. The TS Agent automatically populates this field to 443, the default port on the or On-Prem Firewall Management CenterFMC.
Username and Password	The or On-Prem Firewall Management CenterFMC username and password used to obtain REST VDI privileges on the or On-Prem Firewall Management CenterFMC. For more information about configuring this user, see Creating the REST VDI Role, or

Creating the REST VDI Role

To connect the TS Agent to the Secure Management Center, your Secure Management Center 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*.



Note This task applies to On-Prem Firewall Management Center only.
If you are using Cloud-Delivered Firewall Management Center, see [Get an API Token, on page 9](#) instead.

-
- Step 1** Log in to the Secure Management Center as a user with permissions to create roles.
- Step 2** Click **System** (⚙) > **UsersSystem** > **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 Connection Status, on page 18](#)
- [View TS Agent User, User Session, and TCP/UDP Connection Data on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management Center/FMC, on page 19](#)

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 8](#).

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

- **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 18](#).
- **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 18](#)).
- **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.
	Enter a portion of a username or a complete username in the Filter by Username search field.

Item	Description
	Click to refresh sessions displayed on this tab page.
	<p>Export the following troubleshooting information about the TS Agent as text files:</p> <ul style="list-style-type: none"> • XML file containing TS Agent configuration data • Output from the netstat -a -n -o command • Windows task list • List of running drivers
	<p>Check the box next to one or more sessions to restream those sessions to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. You can use this in the event the user service fails on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC.</p> <p>For example, suppose a user logs in to the TS Agent server after the user service fails on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. 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.</p>

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 Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC for propagation to managed devices.

The Monitor tab page enables you to confirm that the port range was successfully sent to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. Among the reasons why the process might have failed include:

- Network connectivity issues
- 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 8](#).
- 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 Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC, try to restream traffic for that session as discussed in [View Information About the TS Agent, on page 17](#).
- **Success:** The action completed successfully.

View TS Agent User, User Session, and TCP/UDP Connection Data on the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC

Use the following procedure to view data reported by the TS Agent. For more information about the user tables, see the [Cisco Secure Firewall Management Center Administration Guide](#).

-
- Step 1** To access the information in the Secure Management Center, log in.
- Step 2** Access the information in CDO:
- a) Log in to the Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC where you configured the realms targeting the users your server is monitoring.
 - b) Click **Policies > FTD Policies**.
- Step 3** To view users in the Users table, click **Analysis > Users > Users**.
- Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC populates the **Current IP**, **End Port**, and **Start Port** columns if a TS Agent user's session is currently active.
- Step 4** To view user sessions in the User Activity table, choose **Analysis > Users > User Activity**.
- The Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC populates the **Current IP**, **End Port**, and **Start Port** columns if the TS Agent reported the user session.
- Step 5** Log in to your Secure Management Center.
- Step 6** To view TCP/UDP connections in the Connection Events table, click **Analysis > Connections > Events**.
- The Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC 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 21](#)
- [Viewing the Status of the TS Agent Service Component, on page 21](#)
- [Starting and Stopping the TS Agent Processes, on page 22](#)
- [Viewing TS Agent Activity Logs on the Server, on page 22](#)
- [Uninstalling the TS Agent, on page 22](#)

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 Cisco Terminal Services \(TS\) 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 22](#).
-

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 Cloud-delivered Firewall Management Center or On-Prem Firewall Management CenterFMC. 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**.
-