Install and Configure the TS Agent

- Install or Upgrade the TS Agent, on page 1
- Start the TS Agent Configuration Interface, on page 2
- Configure the TS Agent, on page 2
- Creating the REST VDI Role, on page 7

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.
- End all current user sessions as described in Ending a Current User Session.

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-1.2.0.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-1.2.0.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.
- Start the TS Agent as discussed in Starting and Stopping the TS Agent Processes.
- Configure the TS Agent as discussed in Configure the TS Agent, on page 2.

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 FMC as discussed in Creating the REST VDI Role, on page 7.
- If you are already connected to the System and you are updating your TS Agent configuration to connect to a different FMC, you must end all current user sessions before saving the new configuration. For more information, see Ending a Current User Session .
- 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 3.

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 2.

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), and Windows Terminal Server (3389) ports. You must exclude the Citrix MA Client and Windows Terminal Server ports.

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

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

The FMC 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 FMC configured, the test connection to the secondary fails. This is expected behavior. The TS Agent communicates with the active FMC at all times. If the primary fails over and becomes the inactive FMC, the TS Agent communicates with the secondary (now active) FMC.

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 exclud comma-separated list. The TS Agent automatically populates **Reserve Port(s)** with default port values MA Client (2598), and Windows Terminal Server (3389). If you do not exclude ports, applications requiring those ports might fail. **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 sin run several user sessions at a time. This version of the TS Agent supports 29 user sessions by default, up to a maxi user sessions.
Server NIC	This version of the TS Agent supports using a single network interface controlle port translation and server-system communications. If two or more valid NICs a your server, the TS Agent performs port translation only on the address you spec 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 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 co 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 acti **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; howev Agent does not track port usage. System ports are used by the Local System acc local user accounts. (A local user account exists only on the TS Agent server; it corresponding Active Directory account.) You can choose this option to permit t types of traffic: • Permit traffic run by the Local System account (such as Server Message Bl instead of being blocked. The FMC identifies this traffic as coming from th user because the user does not exist in Active Directory. Enabling this option also enables you to successfully test the connection wi if you log in to the TS Agent server using a local system account. • When a user or system session exhausts all available ports in its range, the allows the traffic over ephemeral ports. This option enables the traffic; the FM 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 FMC typically us
Username and Password	The credentials for the connection. • The System requires a username and password for a user with REST VDI p the FMC. For more information about configuring this user, see the *Cisco Se* *Management Center Configuration Guide*.

Creating the REST VDI Role

To connect the TS Agent to the FMC, 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 FMC 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.