Install and Configure the TS Agent

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.
- If you previously installed the TS Agent, uninstall the TS Agent as described in Uninstalling the TS Agent.
- End all current user sessions as described in Ending a Current User Session.

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.

- 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.

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 8.
- 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 .
- 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 3.

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 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.

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)	The port(s) you want the TS Agent to ignore. Enter the ports you want to exclude as a comma-separated list. 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. **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. **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.	Typically one of the following: • `2598,3389` (the Citrix MA Client and Windows Terminal Server ports)
Max User Sessions	The maximum number of user sessions you want the TS Agent to monitor. A single user can run several user sessions at a time. This version of the TS Agent supports up to 199 user sessions.	`199` (the maximum supported value in this version of the TS Agent)

Field	Description	Example
Server NIC	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. 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. **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. **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.	`Ethernet 2 (192.0.2.1)` (a NIC on your server)

Field	Description	Example
System Ports	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. 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. **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. The TS Agent automatically populates the **End** value using the following formula: `( [Start value] + [Range value] ) - 1` If your entries cause the **End** value to exceed the **Start** value of **User Ports**, you must adjust your **Start** and **Range** values.	**Start** set to `1024` and **Range** set to `1000`

Field	Description	Example
User Ports	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. **Note** ICMP traffic is passed without being port mapped. 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. **Note** When the number of ports used exceeds the value of **Range**, user traffic is blocked. The TS Agent automatically populates the **End** value using the following formula: `[Start value] + ( [Range value] * [Max User Sessions value] ) - 1` If your entries cause the **End** value to exceed 65535, you must adjust your **Start** and **Range** values.	**Start** set to `2024` and **Range** set to `200`

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 8.	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.