Integration Guide: SonicOS and Microsoft Remote Desktop Services

May 2019

This document describes how SonicOS is integrated with Microsoft Remote Desktop Services, formerly known as Microsoft Terminal Services, a component of the Windows Server operating system. SonicWall Terminal Services Agent (TSA), installed on a MS Terminal Server, identifies logged in users through a combination of server IP addresses, user names, and domains. It informs SonicOS running on next-generation firewalls for policy enforcement using SonicWall Single Sign-On (SSO) services.

Topics:

About Remote Desktop Services

Remote Desktop Services provides functionality similar to a terminal-based, centralized host, or mainframe, environment in which multiple terminals connect to a host computer. Each terminal provides a conduit for input and output between a user and the host computer. A user can log on at a terminal, and then run applications on the host computer, accessing files, databases, network resources, and so on. Each terminal session is independent, with the host operating system managing conflicts between multiple users contending for shared resources.

Requirements

- SonicOS 5.8/5.9 and 6.1 and above
- UDP port 2259
- Windows Server 2008, 32-bit and 64-bit
- Windows Server 2003, 32-bit and 64-bit
- Windows Server 2012 and 2018, 32-bit and 64-bit

Installing SonicWall TSA on Terminal Server

Install the SonicWall TSA on one or more terminal servers on your network within the Windows domain. The SonicWall TSA must have access to your SonicWall next-generation firewall, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the User

Datagram Protocol (UDP) port number for incoming messages from the appliance. SonicWall TSA is available for download without charge from MySonicWall.

To install SonicWall TSA, perform the following steps:

1 Go to https://mysonicwall.com and sign in with your user name and password.

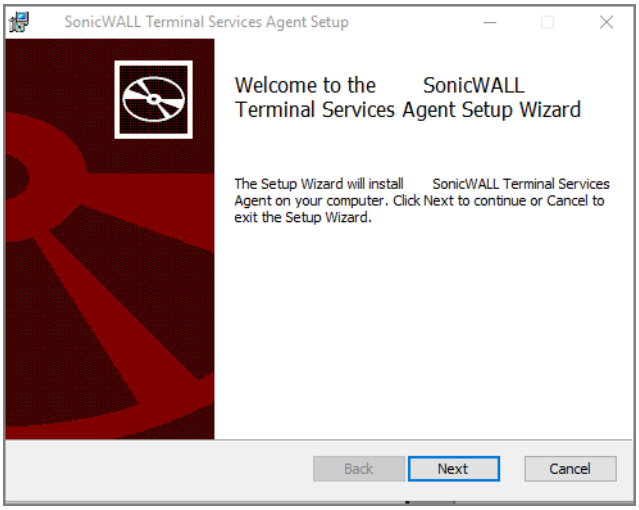
2 In the **Contemporary Mode**, on the left navigation menu, go to **HOME | Downloads > Download Center**.

3 Enter the product name **Terminal Services Agent** in the **Search Firmware & Software** field at the top right.

4 Under the Terminal Services Agent column on the left, download the installation program version you want, depending on your computer:

- SonicWall TSAInstaller32.msi (32 bit, version 3.0.28.1001 or higher)
- SonicWall TSAInstaller64.msi (64 bit, version 3.0.28.1001 or higher)

5 The TSAInstaller.msi file is downloaded. Double click the program to begin installation.

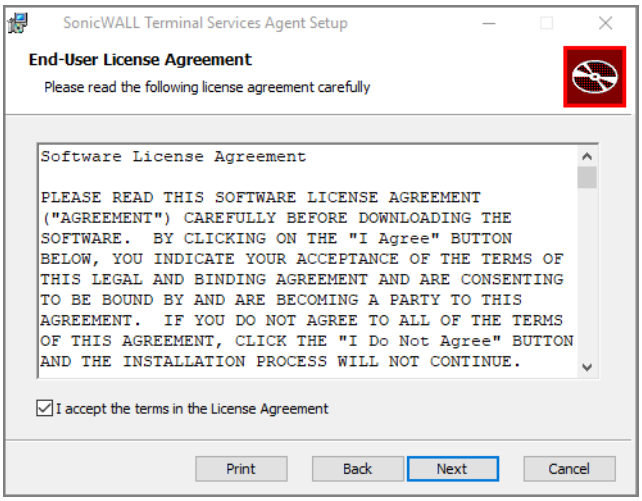


The Setup Wizard will install SonicWall Terminal Services Agent on your computer.

6 Click **Next.**

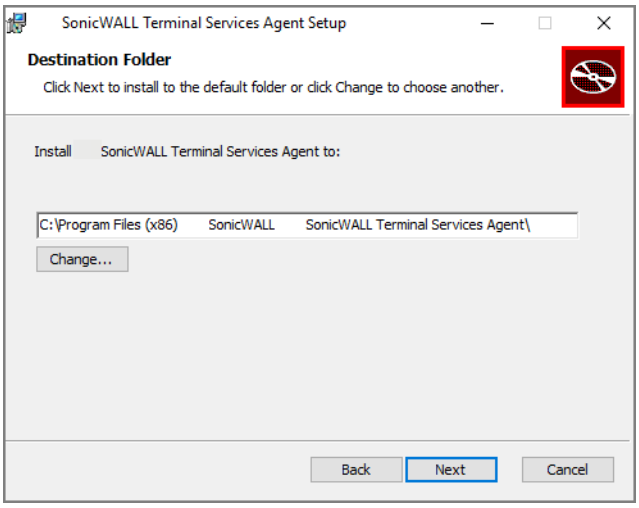
The **End-User License Agreement** displays.

7 Check the box next to **I accept the terms in the License Agreement** and click **Next**.



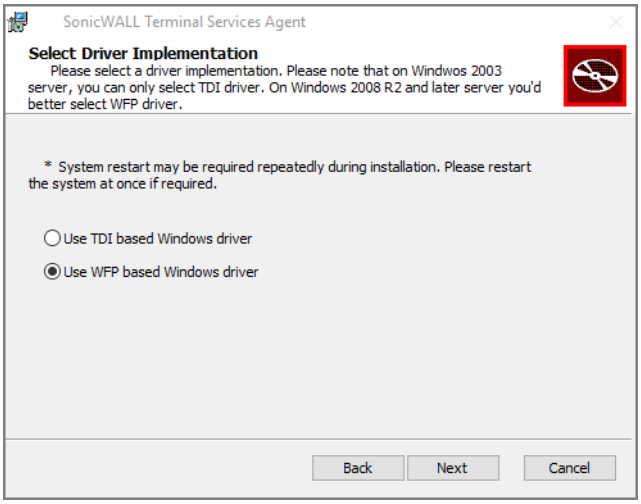
8 On the **Destination Folder** window, select where you want to save your download.

9 Click **Next** to install to the default folder or click **Change** to choose another.



10 On the **Select Driver Implementation** window, choose a driver implementation.

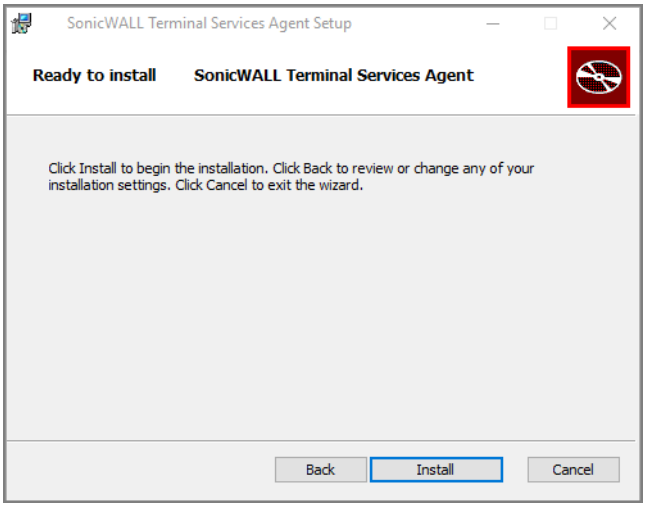
11 On a Windows 2003 server you can only select TDI driver. On a Windows 2008 R2 and later server select WFP driver.



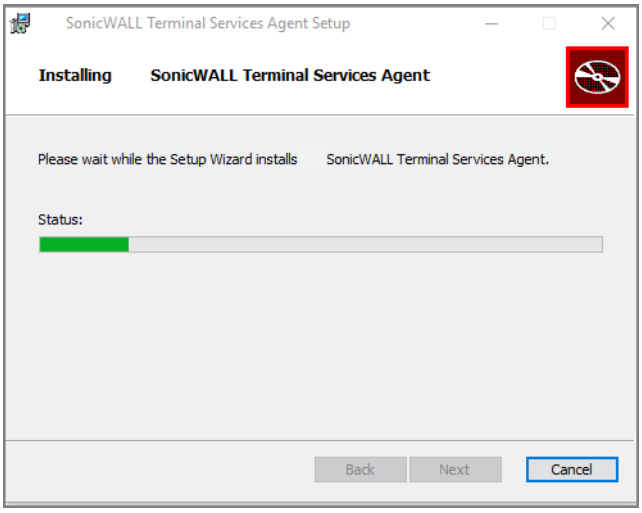
NOTE: You may have to restart your system repeatedly during installation. Restart your system at once if required.

12 Click **Next**.

13 On the **Ready to install SonicWall Terminal Services Agent** window, click **Install**.



Wait while the SonicWall Terminal Services Agent installs. The progress bar indicates the status.



14 When the installation is complete, click **Close** to exit the installer.

15 You must restart your system before starting the SonicWall Terminal Services Agent. To restart immediately, click **Yes** in the dialog box. To restart later, click **No**.

Configuring the SonicWall TSA software

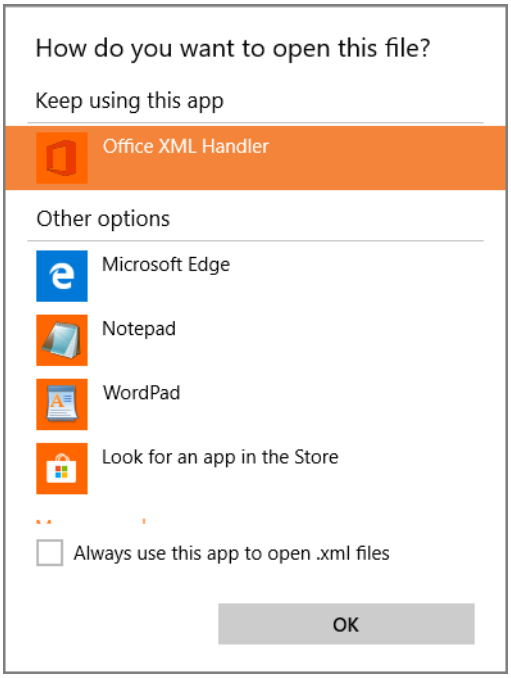
After installing the SonicWall TSA and restarting your Windows Server system, double click the Dell SonicWall TSA folder created by the installer to see the system components:

- Software License Agreement
- swtagent.log file
- swtsas.exe file
- SWTSATSR.exe file
- TSA Confix.xml file.

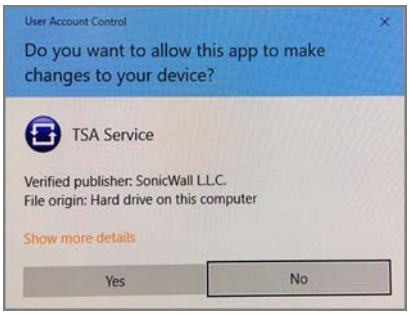
1 Double click the SonicWall TSA folder.

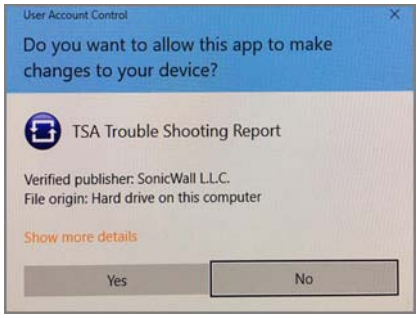
2 Double click the TSAConfix.xml file in the folder.

3 Choose the program to open your configuration file and click **OK**.

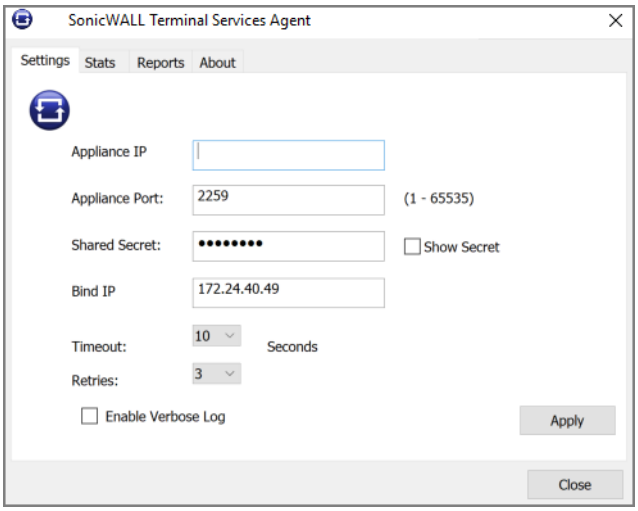


4 Click **Yes** to allow the app to make changes to your device when the two **User Account Control** windows display.





5 In the window that displays, add a SonicWall UTM appliance to SonicWall TSA by clicking the **Settings** tab and typing the IP address of the SonicWall UTM appliance into the **Appliance IP** field.



6 Type the communication port into the **Appliance Port** field. The default port is 2259, but a custom port can be used instead. This port must be open on the Windows Server system.

NOTE: If you have a software firewall running on the terminal server, you may need to open up the UDP port 2259 number for incoming messages from the appliance.

7 Type the encryption key into the **Shared Secret** field. Select the **Show Secret** checkbox to view the characters and verify correctness.

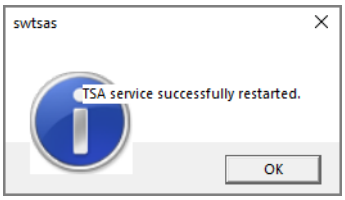
NOTE: The same shared secret must be configured on the SonicWall UTM appliance.

8 In the **Timeout** drop-down list, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is 5 seconds.

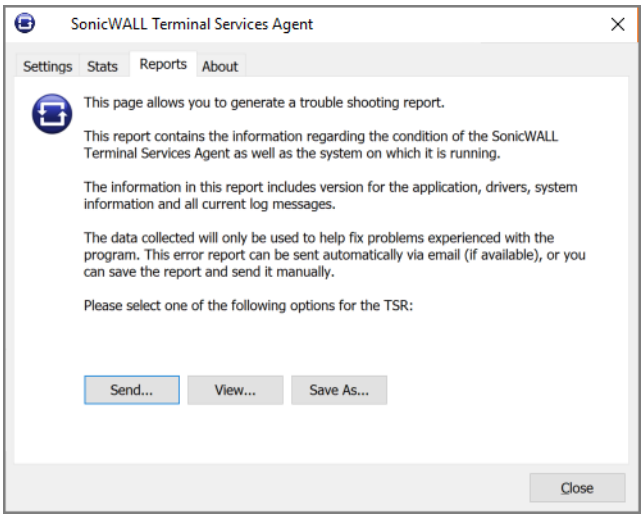
9 In the **Retries** drop-down list, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is 5.

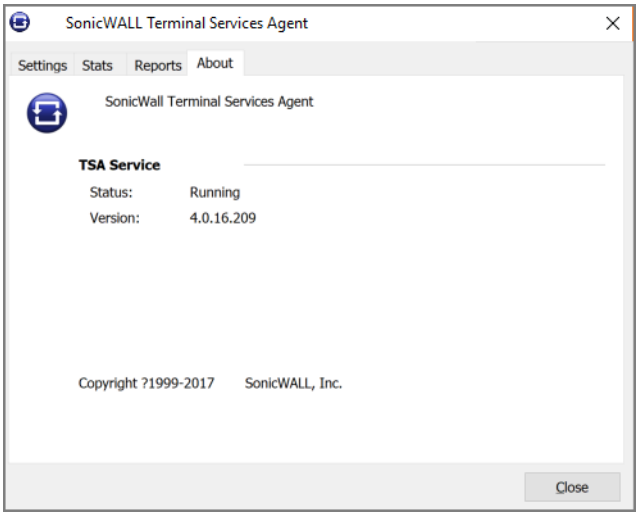
10 To enable full details in log messages, select the **Enable Verbose Log** checkbox. Do this only to provide extra, detailed information in a trouble shooting report. Avoid leaving this enabled at other times because it may impact performance.

11 Click **Apply**. A dialog box indicates that the SonicWall TSA service has restarted with the new settings.



12 Click **OK**.



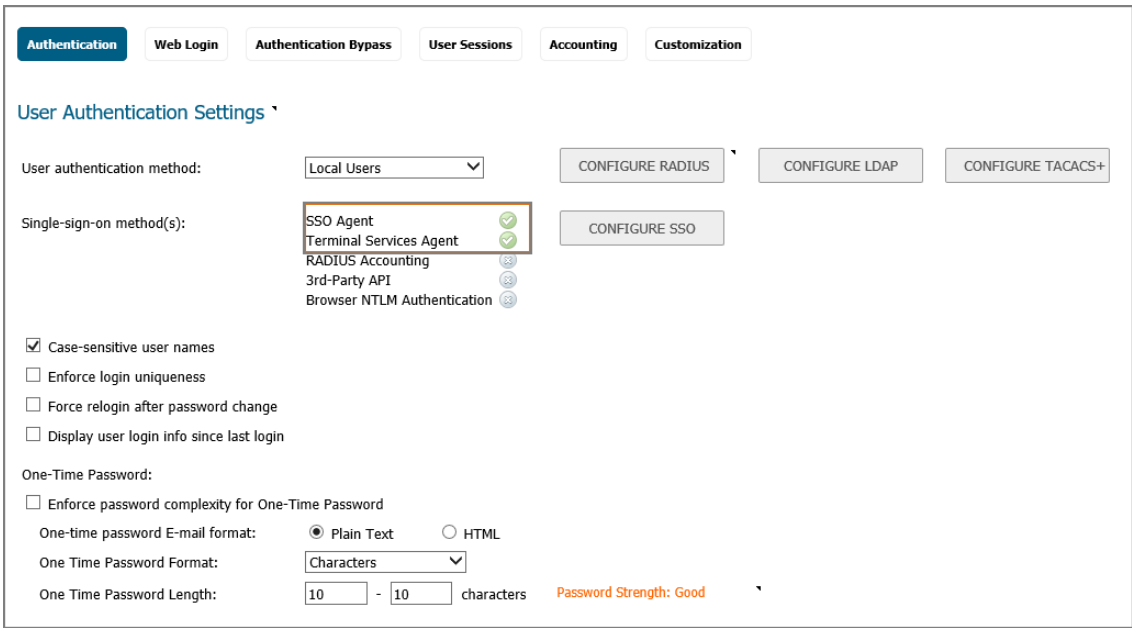


Configuring the TSA settings on the SonicWall

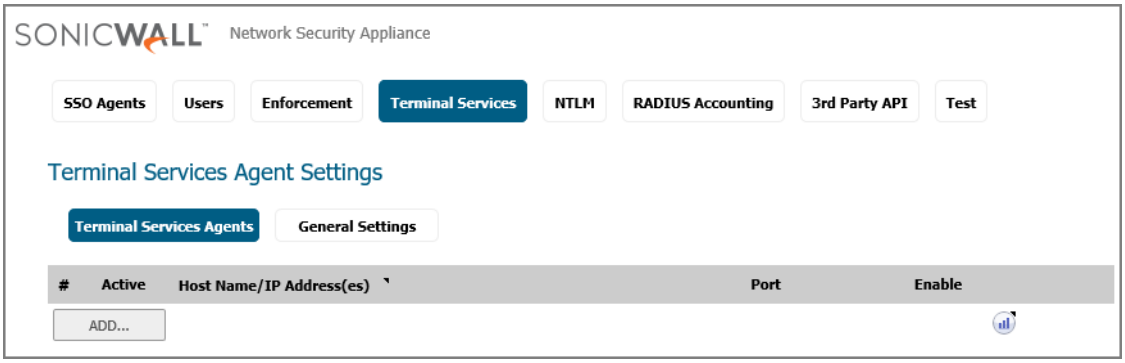
1 Log into your SonicWall security appliance as an administrator.

2 Navigate to **Users > Settings**.

3 In the **Single sign on method** choices menu to the right, select **SSO Agent** and **Terminal Services Agent** for the SSO method**.**



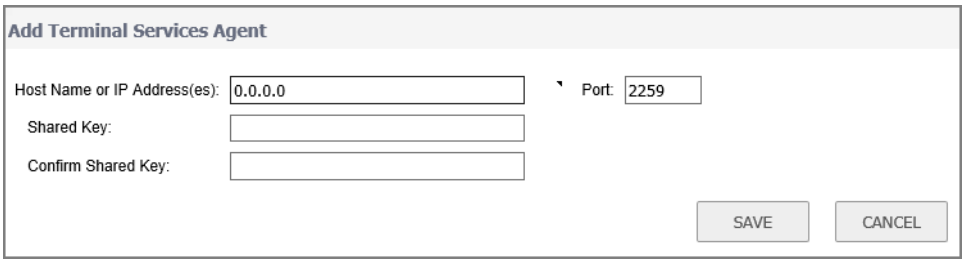
4 Click **CONFIGURE SSO**.



5 In the Authentication Agent Settings page that displays, click the **Terminal Services** tab.

6 Click **ADD**. The page is updated to display a new row in the table at the top, and new input fields in the lower half of the page.

For existing agents, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down. A yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for five minutes or more. Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently doing anything.



7 In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which SonicWall TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list. As you type in values for the fields, the row at the top is updated in red to highlight the new information.

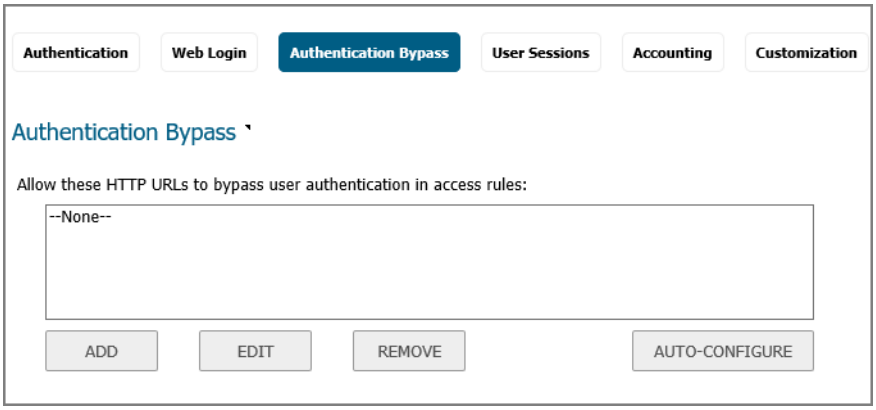
8 In the **Port** field, enter the port number of the workstation on which SonicWall TSA is installed. The default port is 2259. Note that agents at different IP addresses can have the same port number.

9 In the **Shared Key** field, enter the shared key that you created or generated in the SonicWall TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.

10 Click **SAVE**.

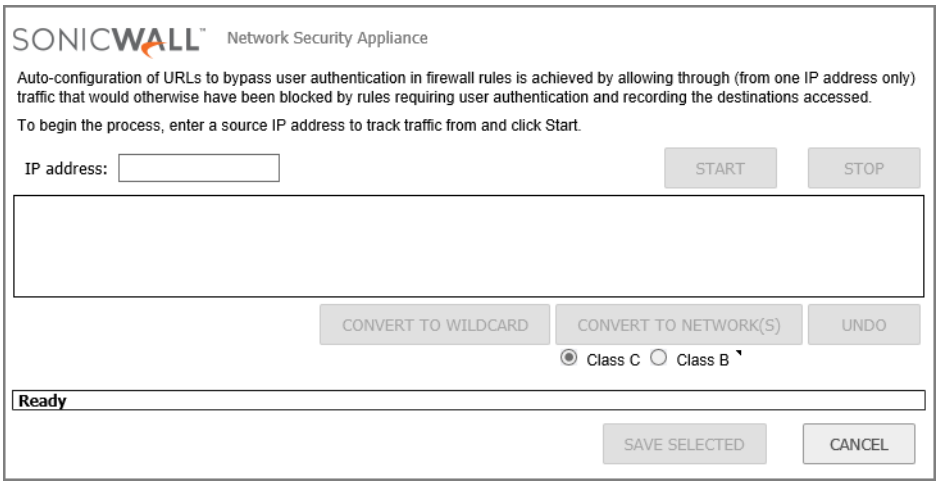
11 Go to **Users > Settings | Authentication Bypass** to allow traffic from services on the terminal server to bypass user authentication. In the text box that displays enter the **HTTP URLs to bypass user authentication in access rules**. This allows traffic such as Windows updates or anti-virus updates, which is not associated with any user login session, to pass without authentication.

12 Click **ADD** to allow access for the HTTP URLs that can bypass user authentication in access rules.



13 Click **AUTO-CONFIGURE** to allow the auto-configuration of URLs to bypass user authentication in firewall rules through one IP address only.

14 Enter a source **IP address** to track traffic from and click **START**.

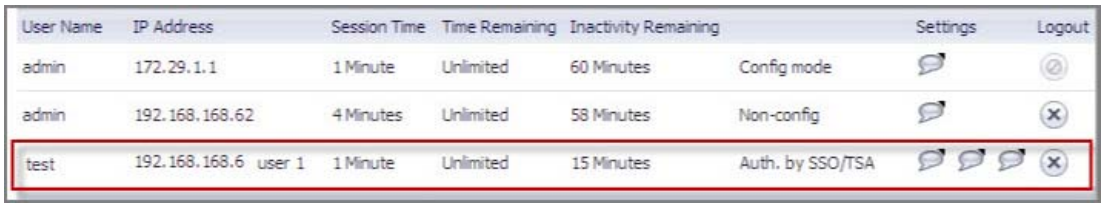


15 If you have multiple agents configured, select the SSO agent or TSA to test from the Select agent to test drop-down list. The drop-down list includes SSO agents at the top, and TSA's at the end under the heading --Terminal Server Agents.

16 Select the Check agent connectivity radio button and then click the Test button. This will test communication with the authentication agent. If testing a TSA, the Test Status field displays the message, and the version and server IP address are displayed in the Information returned from the agent field.

Testing Your Integration

When users log into the Terminal server, each user will be listed separately in the SonicWall appliance on the **Users > Status** page.



To accommodate large installations with thousands of users, SonicWall UTM appliances are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model.

NOTE: For all SonicWall UTM models, a maximum of 32 IP addresses is supported per terminal server.

Encryption of TSA Messages and Use of Session IDs:

SonicWall TSA uses a shared key for encryption of messages between the TSA and the SonicWall UTM appliance when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.

NOTE: The shared key is created in the TSA, and the key entered in the SonicWall UTM appliance during SSO configuration must match the TSA key exactly. The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, it will not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to unlearn these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 5/28/19