SONICWALL®

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
- Requirements
- Installing SonicWall TSA on Terminal Server
- Configuring the SonicWall TSA software
- Configuring the TSA settings on the SonicWall
- Testing Your Integration

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.

👷 SonicWALL Terminal S	ervices Agent Setup - 🗆 🗙
Ð	Welcome to the SonicWALL Terminal Services Agent Setup Wizard
	The Setup Wizard will install SonicWALL Terminal Services Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel

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.

🛃 SonicWALL Terminal Services Agent Setup — 🗌	\times
End-User License Agreement	
Please read the following license agreement carefully	S
Software License Agreement	^
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE DOWNLOADING THE SOFTWARE. BY CLICKING ON THE "I Agree" BUTTON BELOW, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LEGAL AND BINDING AGREEMENT AND ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "I DO NOT AGREE" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE.	1
☑ I accept the terms in the License Agreement	
Print Back Next Car	ncel

- 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.

SonicWALL Termina	al Services Age	ent Setup	-		×
Destination Folder					
Click Next to install to the	e default folder	or click Change to choose	e another.	ľ.	S
Install SonicWALL Terr	minal Services A	Igent to:			
C:\Program Files (x86)	SonicWALL	SonicWALL Terminal S	ervices Agen	t\	
Change					
		Back	lext	Cano	:el

- 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.

SonicWALL Terminal Services Agent	×
Select Driver Implementation Please select a driver implementation. Please note that on Windwos 2003 server, you can only select TDI driver. On Windows 2008 R2 and later server you better select WFP driver.	Jid 🚱
* System restart may be required repeatedly during installation. Please restar the system at once if required.	t
O Use TDI based Windows driver	
Use WFP based Windows driver	
Back Next	Cancel

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.

SonicWALL Tern	ninal Services Agent Setup	_	
Ready to install	SonicWALL Terminal Services	Agent	
Click Install to begin i installation settings.	the installation. Click Back to review or c Click Cancel to exit the wizard.	hange any of you	r
	Back	Install	Cancel

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

17	SonicWALL	Terminal Services Age	nt Setup	_		\times
	Installing	SonicWALL Termin	al Services Age	ent		Ð
	Please wait while	the Setup Wizard installs	SonicWALL Te	erminal Services	Agent.	
	Status:					
			Back	Next	Car	ncel

- 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**.

How	do you want to open this file?
Keep	using this app
٥	Office XML Handler
Other	roptions
е	Microsoft Edge
	Notepad
A	WordPad
Ê	Look for an app in the Store
••	1
	lways use this app to open .xml files
	ОК

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.

😑 s	onicWA	LL Termir	nal Service	s Agent		×
Settings	Stats	Reports	About			
E						
A	Appliance	IP				
A	Appliance	Port:	2259		(1 - 65535)	
S	Shared Se	cret:	•••••	•	Show Secret	
E	Bind IP		172.24.40	.49		
T	Timeout:		10 ~	Seconds		
F	Retries:		3 ~			
	🗌 Enat	ole Verbos	e Log			Apply
						Close

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.

-							
😑 s	onicWA	ALL Termin	al Services Ag	ent			\times
Settings	Stats	Reports	About				
	This pa	ge allows y	ou to generate a	a trouble shooti	ng report.		
	This rep Termina	oort contain al Services	is the information Agent as well as	on regarding the the system on	e condition of the Soni which it is running.	cWALL	
	The info informa	ormation in ation and al	this report inclu current log me	udes version for ssages.	the application, drive	rs, system	
	The dat prograr can sav	ta collected n. This erro e the repor	will only be use or report can be t and send it ma	d to help fix pro sent automatic anually.	oblems experienced wi ally via email (if availal	th the ble), or you	
	Please s	select one o	of the following	options for the	TSR:		
	Ser	nd	View	Save As			
						Close	
						Giose	

🖲 s	onicWALL Ter	rminal Services Agent	×
Settings	Stats Repo	arts About	
8	SonicWall	Terminal Services Agent	
	TSA Service		-
	Status:	Running	
	Version:	4.0.16.209	
	Copyright ?19	99-2017 SonicWALL, Inc.	
		Close	:

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.

Authorities Weblerin Aut	untinetine Russes	A		
Authentication web Login Auth	User Sessions	Customization		
User Authentication Settings `				
User authentication method:	Local Users	CONFIGURE RADIUS	CONFIGURE LDAP	CONFIGURE TACACS+
Single-sign-on method(s):	SSO Agent Terminal Services Agent RADIUS Accounting 3rd-Party API Browser NTLM Authentication @	CONFIGURE SSO		
✓ Case-sensitive user names				
Enforce login uniqueness				
Force relogin after password change				
\square Display user login info since last login				
One-Time Password:				
Enforce password complexity for One	-Time Password			
One-time password E-mail format:	Ilain Text			
One Time Password Format:	Characters 🗸			
One Time Password Length:	10 - 10 characters	Password Strength: Good	•	

4 Click CONFIGURE SSO.

SSO Agents	Users En	oforcement	Terminal Services	NTLM	RADIUS Accounting	3rd Party API	Test
erminal Se	rvices Ager	nt Settings					
erminal Se	vices Agents	nt Settings General Set	tings				

- 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.

Add Terminal Services A	gent			
Host Name or IP Address(es): Shared Key: Confirm Shared Key:	0.0.0.0	• Port: 2259	SAVE	CANCEL

- 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.

uthentication	Web Login	Authentication Bypass	User Sessions	Accounting	Customizatio
thenticatio	n Bypass `				
ow these HTTP	URLs to bypass	user authentication in acc	ess rules:		
None					
None					
None					

- 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.

	curity Appliance		
Auto-configuration of URLs to bypass user a traffic that would otherwise have been block	authentication in firewall rules is ac ed by rules requiring user authenti	hieved by allowing through (from one ication and recording the destinations	IP address only) accessed.
To begin the process, enter a source IP add	ress to track traffic from and click	Start.	
IP address:		START	STOP
	CONVERT TO WILDCARD	CONVERT TO NETWORK(S)	UNDO
		Class C Class B	
Ready			
		SAVE SELECTED	CANCEL

- 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.

User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining		Settings	Logout
admin	172.29.1.1	1 Minute	Unlimited	60 Minutes	Config mode	Ø	0
admin	192.168.168.62	4 Minutes	Unlimited	58 Minutes	Non-config	Ø	×
test	192.168.168.6 user 1	1 Minute	Unlimited	15 Minutes	Auth. by SSO/TSA	000	×

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.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

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