

Sophos UTM Sophos Transparent Authentication Installation Guide

Product version: 1.0 Document date: Wednesday, February 03, 2016

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of Sophos Limited. Translations of this original manual must be marked as follows: "Translation of the original manual".

© 2016 Sophos Limited. All rights reserved.

http://www.sophos.com

Sophos UTM, Sophos UTM Manager, Astaro Security Gateway, Astaro Command Center, Sophos Gateway Manager, Sophos iView Setup and WebAdmin are trademarks of Sophos Limited. Cisco is a registered trademark of Cisco Systems Inc. iOS is a trademark of Apple Inc. Linux is a trademark of Linus Torvalds. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to nsg-docu@sophos.com.

Contents

1 Features Overview	vii
1.1 Operating Principle of STAS	vii
2 Prerequisites	ix
2.1 Configuring AD Controller	ix
2.2 Activating STAS	x
3 Installation	xiii
3.1 Downloading STAS	xiii
3.2 Installing STAS	xiv
4 Configuration	xviii
4.1 Configuring STAS Agent	xviii
4.2 Configuring STAS Collector	xx
4.3 Showing Live Users	xxiii
4.4 Starting STAS Service	
5 Settings on AD Server	xxvi
5.1 Activating Event Logging	xxvi
5.2 Defining NetBIOS Domain Data	xxvii
6 Connectivity Test	xxix
6.1 STAS Agent and STAS Collector	xxix
6.2 STAS Collector and Sophos UTM	xxxi
6.3 STAS Collector and Workstation	
6.3.1 WMI Verification	
6.3.2 Registry Read Verification	xxxv

1 Features Overview

Sophos introduces clientless Single Sign On as a Sophos Transparent Authentication Suite (STAS). This chapter gives an overview of its features and functionality.

Sophos Transparent Authentication Suite eliminates the need to remember multiple passwords as the user logs on to Sophos UTM automatically when he logs on to Windows with his Windows username and password. Moreover, it eliminates the installation of SSO clients on each work-station. Hence, it provides high ease-of-use to end-users and higher levels of security in addition to lowering operational costs involved in client installation.

STAS consists of two main components:

- STAS Agent (on the AD server)
- STAS Collector (on any machine)

STAS Agent: Monitors user authentication requests on the domain controller and sends information to the Collector for Sophos authorization.

STAS Collector: Collects user authentication requests from multiple agents, processes the requests and sends them to Sophos UTM for authorization.

1.1 Operating Principle of STAS



STAS Operating Principle

1. The user logs on to the Active Directory domain controller from any workstation in the LAN. The domain controller authenticates the user credentials.

Access is only granted for users logged onto the domain. Users who are logged into a workstation directly (or locally) but not logged in as a domain user will not be authenticated and are considered as "unauthenticated" users.

- 2. The STAS Agent captures and communicates this authentication process to the STAS Collector over the default TCP port (5566) in real time.
- 3. The STAS Collector registers the user in the local database and communicates the user's IP address and username to Sophos UTM over its default UDP port (6077).
- 4. Sophos UTM queries the Active Directory domain controller to determine the user's group membership and registers the user in the Sophos UTM database.
- 5. The STAS Collector regularly polls all workstations available in its user map to check if the same user is still logged in.

2 Prerequisites

Before STAS can be configured, some settings have to be made on Sophos UTM.

The following topics are included in this chapter:

- Configuring the AD controller
- Activating STAS

2.1 Configuring AD Controller

One central element of Sophos Transparent Authentication Suite is the domain controller hosting the STAS Agent. So, before installing STAS, the Active Directory domain controller has to be configured.

To configure the domain controller, proceed as follows:

- 1. Log in to the WebAdmin console as administrator.
- 2. Navigate to Definition & Users > Authentication Services > Servers.
- 3. Click New Authentication Server.
- 4. As backend, select Active Directory.

🔎 search	Authentication Services						
Dashboard	Global Settings Servers	Single Sign-O	n 🔰 🙆 One-tim	ne Pa Advanced			
Management	+ Now Authoritication Comm		Search		Find		
Definitions & Users	T New Automication Server			·]			(()
Network Definitions					C	isplay: 10 💌	1-1 0
Service Definitions	Add Authentication Server		X	C Action 🗮 🔻	Sort by: Po:	ition asc 💌	
Users & Groups	Backend	Active Director	y 🔳	🗆 📝 Edit	1 a	lirectory	0
Client Authentication	Position:	Тор	•	× Delete	Host w (10.8.3	'ewe 2.222:389)	Base DN
Authentication Services	Server:		DN 🚔 🕇	Clone			
Interfaces & Routing	881						
Network Services	Port	389					
Network Protection	Died DNI:						
Web Protection	Bind DN.						
Email Protection	Fassword.	Teat					
Advanced Protection	lest server settings	lest					
Endpoint Protection	Base DN:						
Wireless Protection	Usemame:						
Webserver Protection	Password:						
RED Management	Authenticate example user	Test					
Site-to-site VPN							
Remote Access		Save	× Cancel				
Logging & Reporting							
Support							
Log off							
Log off							

Definition of new Authentication Server

Fill in the remaining fields as described in the online help of the WebAdmin console (for help, click the "?" button).

2.2 Activating STAS

To use STAS, it first must be enabled and a collector machine has to defined.

To enable STAS, proceed as follows:

- 1. Navigate to Definition & Users > Client Authentication.
- 2. Switch to the Sophos Transparent Authentication Suite tab.
- 3. Under "STAS Status", activate the toggle switch.
- 4. Click New STAS Collector.
- 5. As port, select STAS Collector.

🔎 search	Client Authen	ticatio	n												
Dashboard	Global	8 CI	ient Authe		📀 Sop	hos Tra									
Management	STAS etatue	-													
Definitions & Users		The	Sonhoe 1	Franchar	ont Aut	henticatio	n Sui	ta n	narom co	he fetr	hed from	the LITM S	upport Do	woloade nade	
Network Definitions		me	auprius i	ranspar	entAut	nenticatio	au	te p	ugrani cai	i be lett	ineu ironi	The OTH S	opportoc	iwilloads page	
Service Definitions	+ New ST/	S Col	lector					۶	earch			Find			« »
Users & Groups													Display	10 💌	1-1 of
Client Authentication	Add STAS C	ollecto	r				×	Π	Action	= +	Sort by	Name as			
Authentication Services	Nama				_		-		📝 Edit	-	wewe:	STAS Colle	ctor		0
Volwork Carvican	Name.	DAV							× Delete	,	Host	wewe			
Vetwork Brotection	HUSL	DIVI							Clone		Port	6677			
Neh Protection	Port	Π,	STAS C	ollector		-	+				1 011	0077			
Empil Protection	Comment														
Entail Protection				√ s	iave	× Can	cel								
Terde sist Destaction															
Enapoint Protection															
Valeness Protection															
Prebserver Protection															
Pito to pito (@NI															
orging & Reporting															
Bunnort															
anoff															
_0g 0ii															

Definition of STAS Collector

6. Fill in the remaining fields as described in the online help of the WebAdmin console (for help, click the "?" button).

3 Installation

This chapter provides a step-by-step guide to include Sophos Transparent Authentication Suite to Sophos UTM.

The following topics are included in this chapter:

- Downloading STAS
- Installing STAS

3.1 Downloading STAS

The Sophos Transparent Authentication Suite program can be fetched from the Sophos UTM Support Download page.

To download the program, proceed as follows:

- 1. Go to https://www.sophos.com/en-us/support/utm-downloads.aspx.
- Under the section "Sophos Tranparent Authentication Suite (STAS)", download the STAS installer.

Ditei Bearbeiten Anlicht Chronik Leonzeichen bi	Aur Bar				1016			
C open office download - 01_ A S OTM Sup	postcounters x 4							
Multi-acyte [] Erts Schers [] Sussand Stat	R was the Galaxy		Ų	- C				
Contraction of the state of addition and	E				-			
	SUPHUS	PRODUCTS LABS	PARTNERS COMPANY	SUPPORT I G	Q			
		Overview Support Par	keges Download Decume	reation Training 🐸 Corea				
	Sophos Support							
	UTM Support Dov	vnloads						
	These downloads are far installation support versions can be found on the Legacy UTM do	for existing partners and customers o writoads page (requires a MySophos o	nly. Use the links below to gain access cosunt).	s to the full software files. Older legacy				
	If you are looking for Sophos XG Firewall	downloads then please click here.						
	If you and internetation (Suphose UTM but haven't yet purchased &, follow the United signing find internal. Atternatively, if you want a free trial, of the Suphos Firewall, products then follow the link to spin up for a Sochos Firewall, Sochos Firewall, Manager et Sochos Firewall, and							
	Sophos UTM							
	Complete unified threat management for you	ar network. Existing customers may de	wnload the full ISO below for installat	ian support.				
	Sophos UTM Smart Installer							
	Platform	Version	File	Checksum				
	UTM v9 hardware appliance		wi-9.350-33.im					
		9.351-3.1	Download V	mdS				
			wi937-51 in					
		9.317-5.1	Developed and	m#5				
			Downcoud					
			UTM_Hardware_x8.20+123					
a 🛆 🐃 n 📦	X X 🕅				- N N 4 - 104			
	× <u>A</u> 🔛				- 10 10 10/3			

UTM Support Downloads

3. Follow the on-screen instructions to install STAS on the Active Directory domain controller. Administrative right is required to install STAS.

3.2 Installing STAS

On executing the STAS installer file (STAS [version No.] Release.exe) the setup wizard welcome screen appears.



STAS Welcome screen

To start the installation, proceed as follows:

1. Click Next to proceed.

A window is displayed asking for the destination to install the program.

- 2. Specify the installation folder:
 - 1. Click Next to install STAS at the default location.
 - 2. Click Browse to change the location and specify a destination folder.
 - 3. Once the destination is selected, click Next.

For installation, at least 4.1 MB of free disk space is required. The client will not be installed, if there is not enough disk space.

- 3. Specify the Start menu folder:
 - 1. Click Next to create a shortcut of the program at the default location.
 - 2. Click Browse to change the location and specify a destination folder.
 - 3. Once the destination is selected, click Next.
- 4. Select additional tasks: Enable the respective checkboxes if you want to create a STAS icon on the desktop or a Quick launch icon.
- 5. Click *Install* to install the Sophos Transparent Authentication Suite at the selected location or click *Back* to change the location.
- 6. Select the type of setup:

Ę	Sophos Transparent	Authentication Suite 🛛 🗙	
1	Type of Setup		
	SSO Suite	Installs all Sophos SSO Suite components on this machine.	
	C STA Collector	Installs only STA Collector on this machine.	
	C STA Agent	Installs only STA Agent on this machine.	
		Next Cancel	

Type of Setup

 Select STA Agent if you want to monitor user authentication requests on the domain controller and send information to the Collector for authorization on Sophos UTM.

- Select STA Collector if you just want to collect user authentication requests from multiple agents, process the requests and send them to Sophos UTM for authorization.
- Select SSO Suite to install both of the above components. By default, the entire SSO Suite is installed.

Click Next to proceed.

7. Specify the administrator user account:

phos Transparent Auth	entication Suite 🛛 🗙
The user account on which	you want to launch the service
Please enter the user acco administrator user.	unt's username and password. This must be an
User name must be in form accout please enter .\User	DomainName\UserName. If you want to use local user Name
User Name	[
Password	
Confirm Password	
	Back New Concel

User Account Setup

Specify the username and the password for the user for which you want to launch the service. This user must have administrative rights for the machine on which you are installing STAS.

Sophos Transı	oarent Authen	tication Suite		×
Press Finish I	to complete insta	llation.		
Attention: P Sophos Trar Windows fin	lease ensure tha Isparent Authent ewall.	t the communic ication Client is	ation between Soph not blocked by the	os and
		Back	Finish	Cancel

Once the installation is completed successfully, the following screen is displayed.

- 8. Click Finish to exit.
- 9. Check for the Sophos Transparent Authentication Suite from **Start > All Programs**. If installed successfully, this tab is added to the Start menu.

After the successful installation, you need to configure STAS on your AD server.

4 Configuration

Once the Sophos Transparent Authentication Suite is installed, it has to be configured on the AD server it is to be applied. This chapter describes the two-steps process to configure STAS on the AD server.

The following topics are included in this chapter:

- Configuring the STAS Agent
- Configuring the STAS Collector
- Showing Live Users
- Starting the STAS Service

4.1 Configuring STAS Agent

To configure the STAS Agent, proceed as follows:

- 1. Launch the program from *Start > All Programs > STAS > Sophos Transparent Authentication Suite* or from the Desktop shortcut.
- 2. Switch to the STA Agent tab and configure the parameters as given below:
 - 1. In the field "STA Agent Mode", select the workstation communication method Recommended: EVENTLOG

In case of "Eventlog", the agent has to be installed on the domain controller, in case of "Netapi", the domain controller can be selected.

2. In the section "Monitored Network", specify the networks to be monitored for user authentication. Multiple networks can be added.

Sophos Transparent Authentication Suite		x
General STA Agent STA Collector Exclusion List	Advanced About	1
STA Agent Mode: EVENTLOG	•	
Monitored Networks		
192.168.1.0/24	I	
	A00	
	Edit	
	Remove	
Domain Controller Polling		
Specify the domain controller to be polled:		
	Add	
	Edit	
	Remove	
Collector List		
Specify the other STA collectors to be serverd:		
	Add	
	Edit	
	Remove	
(L) Language OK Cancel	Apply]

Configuration of STAS Agent

- Add the collector(s). The list order defines the precedence: The top collector gets the information from the agent.
- 4. Click Apply.

4.2 Configuring STAS Collector

To configure the STAS Collector, proceed as follows:

- 1. Switch to the STA Collector tab and configure the parameters as given below:
 - 1. In the section "Sophos Appliances", specify the UTM IP address to which the STAS Collector has to forward user information.
 - 2. In the section "Workstation Polling Settings", specify the method for polling user information. Available options are:
 - WMI
 - Registry Read Access

Default: WMI

3. In the section "Logoff Detection Settings", enable Logoff Detection if you want to monitor user log-offs.

If enabled, specify the Detection Method (either pinging the workstation or polling through WMI or Registry Read Access).

Default: disabled

If enabled, it is recommended to use the WMI detection method.

If you enable *Logoff Detection Settings*, ensure that the firewalls on all workstations are configured to allow traffic to and from the domain controller.

- If ping is selected as log off detection method, ensure that the workstation firewall allows ping packets.
- If WMI polling method is selected, ensure that the workstation firewall allows traffic over UDP port 135.
- Dead Entry Timeout: Specify if you want a user to be logged off from the UTM after the mentioned time, even when the Logoff Detection for the users is disabled.

- In the section "Application Port", specify the UDP port on which the STAS Collector is to listen for requests from Sophos UTM. Default: 6677
- Specify the TCP port on which the STAS Collector is to listen for requests from remote STAS Agents. Default: 5566

Make sure that the AD server has TCP port 5566 open to communicate with the STAS Collector. If the STAS Collector also runs on the AD domain controller, UDP port 6677 must be open to communicate with Sophos UTM.

Sophos Transparent Authentication Suite	X
General STA Agent STA Collector Exclusion List Advance	ed About
Sophos Appliances	
192.168.1.1 A	dd
E	
Ren	nove
- Workstation Polling Settings	
Logoff Detection Settings	
Enable Logoff Detection	
Detection Workstation polling	v
Detection Interval: 605 Seconds (600-	3600)
Dead entry timeout 0 Hours (0 is disa	abled)
Application Port	
Listening to the Sophos appliances on Port	6677
Listening to the remote STA Agents (if any) on Port	5566
(L) Language OK Cancel	Apply

Configuration of STAS Collector

3. Click Apply.

4.3 Showing Live Users

As the STAS Collector is regularly polling user information from its user map administrators have the possibility to check which users are online at a specific point in time.

To see live users, proceed as follows:

- 1. Switch to the Advanced tab.
- 2. Click the Show live Users button.

Sophos Transparent Authentication Suite	Live Users	×
eneral STA Collector Exclusion List Advanced About	Find Refresh	
Logging Loge KB 10 Show Live Uses 10-25) Log Level Debug V Vew Log Vew Log Vew Log Vew Log Vew Log Show Live Log KB Log	Utermanne Doman Workstaton IP Logged-in Time Logon Type Administrator w20127_mgpa.text 0.0.932.222 Fri Dec 11 2015 00:550:20 2	
Backup / Pastne Backup Configuration Backup New Peetore Configuration Upload and Restore		
Troublehooding STAS Poling Millies Will Vertication Registry Read Vertication Text Vertication Text		
Test Connectivity Sophoo Test STAS Agent Test STAS Collector Test		
Configuration Sync Configuration Sync (J) Language OK Cancel Apply		

Show Live Users

This list is identical with the one shown on the *Global* tab in the "Client Authentication" section of Sophos UTM.

4.4 Starting STAS Service

Finally, you can start the STA Agent via the *General* tab on the Sophos Transparent Authentication Suite and check the settings made for the monitored domains. To start the STAS Agent, proceed as follows:

- 1. Switch to the General tab.
- 2. Start the STAS Agent service.

ohos Transparent Authentic	ation Suite		
eneral STA Agent STA Collec	ctor Exclusion List Advanced About		
Statue			
Current Status of STA Agent:	Stopped Start		
	Jian		
- Administrative Credentiale			
Change uppr account on which			
launched	Update		
Monitored Domains			
Following domains are being mo	onitored		
Domain Type	Microsoft Active Directory		
NetBIOS Name:	CELAB		
Fully Qualified Domain Name:	celab org		
Sophos Appliances			
Following Sophos Appliances a	ire being served		
Application Port			
Listening to the Sophos applian	ices on Port 6677		
Listening to the remote STA Agents (if any) on Port 5566			
(
(L) Language OK	Cancel Apply		

Start STAS Service

After configuring STAS on the AD server, you need to make some settings on the AD server.

5 Settings on AD Server

Several settings are required on the AD server to run Sophos Transparent Authentication Suite. This chapter lists the necessary procedures.

The following topics are included in this chapter:

- Enabling Security Event Logging
- Determining NetBIOS, FQDN, and Search DN

5.1 Activating Event Logging

To enable security event logging, proceed as follows:

- Go to Start > Control Panel > System and Security > Administrative Tools > Local Security Policy to view the security settings.
- Navigate to Local Policies > Audit Policy and double click on Audit account logon events to view the "Audit account logon events Properties" window.

1

3. Enable Audit of Success and Failure logon events, as shown in the screen below.

Audit account logon events Properties	? ×
Local Security Setting Explain	
Audit account logon events	
Audit these attempts:	
🗖 <u>F</u> ailure	
This setting might not be enforced if othe override category level audit policy. For more information, see <u>Audit account</u>	er policy is configured to <u>logon events</u> . (Q921468)
ОК	Cancel <u>Apply</u>

Audit Account Logon Events

5.2 Defining NetBIOS Domain Data

To determine the NetBIOS name, FQDN and search DN, proceed as follows:

 Go to Start > Programs>Control Panel > System and Security > Administrative Tools > Active Directory Users and Computers. Right-click the required domain and go to the *Properties* tab. Search DN will be based on the FQDN. In the given example FQDN is w2012r2.nsgqa.test, so the search DN will be DC=w2012r2, DC=nsgqa, DC=test.

		Active Directory	Users and Computers	= 0 ×
File Action View Help				
🗢 🤿 📷 🖬 🖾 🙆 🖬 🖬	🗏 📚 🛍 🍸 🔟 😵			
Active Directory Users and Computers [Saved Queries A Ward Queries Billion D D D	Name Saved Queries w2012r2.nsgqa.test	Type •	Description Folder to store your favo	
 ForeignSecurity-Fineingshit LettArdforund Managed Service Accounts Pregiam Data Pregiam Data Pregiam Data Pregiam Data Wars Wars TPM Devices 		W2012/2 regi General Managed 6y Object 5 W20122/ragpa test Demain name (pre-Windows 2000) W201782 Demotytion: United Server 2012 R2 Forest functional level: Windows Server 2012 R2	atest Properties ? X	
< III >				
		1a. 🥪 🕼		🙀 🖾 🕞 🧐 🍙 DEU 13:06

Active Directory User Configuration

6 Connectivity Test

Sophos Transparent Authentication Suite(STAS) allows administrators to test the connectivity of a Sophos appliance, STAS Agent and STAS Collector with the AD server where the STAS Agent/Collector/Suite is installed.

This chapter describes how to test the connectivity between STAS and external devices as well as between the STAS components.

The following topics are included in this chapter:

- Testing the connectivity between STAS Agent and STAS Collector
- Testing the connectivity between STAS Collector and Sophos UTM
- Testing the connectivity between STAS Collector and workstation

6.1 STAS Agent and STAS Collector

To test the connectivity between the STAS Agent (installed on the domain controller) and the STAS Collector, proceed as follows:

- 1. Launch STAS and switch to the *Advanced* tab.
- 2. Under the "Test Connectivity" section, specify the IP address of the STAS Collector.

Sophos Transparent Authe	ntication Suite	X
General STA Agent ST	A Collector Exclusion List	Advanced About
Logging Log File Size (MB	10	Show Live Users
Log Level	Debug 👻	View Log View Logging Events
Backup / Restore		
Backup Configuration	Backup Now	
Restore Configuration		Browse
	Upload and Restore	
Troubleshooting STAS Polling Utilities		
WMI Verification		Test
Registry Read Verification		Test
Test Connectivity		
Sophos		Test
STAS Agent		Test
STAS Collector	172 . 16 . 16 . 21	Test
Configuration Sync		
Configuration Syr	nc	View Sync Logs
(L) Language	OK Cancel	Apply

3. Click *Test* to test the connection with Sophos. If the connection is successful, the following screen is displayed



If the connection fails, the following screen is displayed:

ConfigSTAS 📃	x
Test Connection failed.	
ОК	

6.2 STAS Collector and Sophos UTM

To test the connectivity between Sophos Transparent Authentication Suite (installed as a collector/suite on the Windows desktop) and Sophos UTM, proceed as follows:

- 1. Launch STAS and switch to the Advanced tab.
- 2. Under the "Test Connectivity" section, specify the IP address of the Sophos UTM.

Sophos Transparent Authentication Suite	
General STA Agent STA Collector Exclusion List Advanced About	
Log File Size (MB 10 Show Live Users 10-25)	
Log Level Debug View Log View Log View Log	s
Backup / Restore Backup Configuration Backup Now	
Restore Configuration Browse	
Troubleshooting STAS Polling Utilities	
WMI Verification	
Verification · · · · lest	
Sophos 172 . 16 . 16 . 25	
STAS Agent Test	
STAS Collector lest	
Configuration Sync Configuration Sync View Sync Logs]
(L) Language OK Cancel Apply	

3. Click *Test* to test the connection with Sophos UTM. If the connection is successful, the following screen is displayed



If the connection fails, the following screen is displayed:

ConfigSTAS	×
Test Connection fa	iled.
	ок

6.3 STAS Collector and Workstation

You can check the connectivity between a workstation and the STAS Collector in two ways:

- WMI Verification
- Registry Read Verification

6.3.1 WMI Verification

Use this method only if the Workstation Polling Method is set to "WMI".

To check the connectivity using WMI, proceed as follows:

- 1. Launch STAS and switch to the Advanced tab.
- 2. In section "Troubleshooting" in the field *STAS Polling Utilities* enter the IP address of the workstation.
- 3. Click Test.

Sophos Transparent Authentication Suite	×
General STA Agent STA Collector Exclusion List Advanced About	
	٦
Log File Size (MB 10 Site Viel Size)	
Log Level Debug View Log	
Backup / Restore	21
Backup Configuration Backup Now	
Restore Configuration Browse	
Upload and Restore	
Troubleshooting	
WMI Verification 10 . 10 . 10 . 5	
Registry Read · · · · Test	
Test Connectivity	
Sophos · · · Test	
STAS Agent Test	
STAS Collector · · · Test	
Configuration Sync Configuration Sync View Sync Logs	
(L) Language OK Cancel Apply	

To perform a successful WMI verification, access to UDP port 135 must be allowed by the workstation firewall.

6.3.2 Registry Read Verification

Use this method only if the Workstation Polling Method is set to "Registry Read Access".

To check the connectivity using Registry Read Access, proceed as follows:

- 1. Launch STAS and switch to the Advanced tab.
- 2. In the section "Troubleshooting" in the field *STAS Polling Utilities* enter the IP address of the workstation.

3. Click Test.

Sophos Transparent Authe	ntication Suite	×
General STA Agent ST	A Collector Exclusion List	Advanced About
Logging		
Log File Size (MB 10-25)	10	Show Live Users
Log Level	Debug 🔹	View Log
Backup / Restore		
Backup Configuration	Backup Now	
Restore Configuration		Browse
	Upload and Restore	
Troubleshooting STAS Polling Utilities		
WMI Verification		Test
Registry Read Verification	10 . 10 . 10 . 5	Test
Test Connectivity		
Sophos		Test
STAS Agent		Test
STAS Collector		Test
Configuration Sync	20	View Sync Logs
(L) Language	OK Cancel	Apply

6 Connectivity Test

To perform a successful Registry Read verification, the remote registry service should be started on the workstation.

To check the service:

- 1. Launch Run and open services.msc.
- 2. Select Remote Registry and make sure that the service is started.