Configure External Authentication and Authorization via LDAPS for Secure Network Analytics Manager Access

Contents

Introduction **Prerequisites** Requirements **Components Used** Configure Step A. Log into the AD domain controller and export the SSL certificate used for LDAP. Step B. Log into the SNA Manager to add the certificate of the LDAP server and the root chain. Step C. Add the LDAP external service configuration. SNA Version 7.2 or later SNA Version 7.1 Step D. Configure Authorization settings. Local Authorization Remote Authorization via LDAP Verify **Troubleshoot Related Information**

Introduction

This document describes the basic configuration of a Secure Network Analytics Manager (formerly Stealthwatch Management Center) version 7.1 or later to use external authentication and, with version 7.2.1 or later, to use external authorization with LDAPS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Network Analytics (formerly Stealthwatch)
- General LDAP and SSL Operation
- General Microsoft Active Directory management

Components Used

The information in this document is based on these components:

- Cisco Secure Network Analytics Manager (formerly SMC) version 7.3.2
- Windows Server 2016 configured as Active Directory Domain Controller

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step A. Log into the AD domain controller and export the SSL certificate used for LDAP.

- 1. For Windows Server 2012 or later select **Run** from the Start menu, then enter **certIm.msc** and continue with step **8**.
- 2. For older Windows Server versions select **Run** from the Start menu, and then enter **mmc**.
- 3. From the File menu, select Add/Remove Snap In.
- 4. From the Available snap-ins list, select **Certificates**, then click **Add**.

liable snap-ins:	Vendor	^	Console Root	Edit Extensions.
	Manage & Car			
Active Directory Do	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			
Active Directory Use	Microsoft Cor			Mauritz
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Microsoft Cor		Add >	11012.00111
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
[®] Disk Management	Microsoft and	~		Advanced
cription:				

- 5. In the Certificates snap-in window, select Computer account, and then select Next.
- 6. Leave Local computer selected, and then select Finish.
- 7. In the Add or Remove Snap-in window, select OK.
- 8. Navigate to Certificates (Local Computer) > Personal > Certificates



9. Select and right-click the SSL certificate used for LDAPS authentication on your domain controller and click **Open**.

10. Navigate to the Details tab > click Copy to File > Next

Certi General	ficate Details	Certification P	ath			>
Show:	<all></all>			\sim		
Field Ve Se Sig	rsion rial numbe pature al pature he	er gorithm ash algorithm	Value	-		^
Va Va	uer lid from lid to hiect		2			~
			Edit Prope	erties	Copy to	File
					E	ОК

- 11. Ensure that **No, do not export private key** is selected and click **Next**
- 12. Select Base-64 encoded X.509 format and click Next.

Expo (rt File Format Certificates can be exported in a variety of file formats.
5	Select the format you want to use:
	O DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78) Include all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	 Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	Microsoft Serialized Certificate Store (.SST)

13. Select a location to store the certificate, name the file and click **Next**.

🚰 Certificate Export Wiza	ard	
File to Export Specify the name of t	he file you want to export	
File name:		
 Committee and an 	LDAPSidcertificate.cer	Browse

- 14. Click **Finish**, you must get a "The export was successful." message.
- 15. Go back to the certificate used for LDAPS, then select the **Certification Path** tab.

16. Select the Root CA issuer on top of the certification path and click View Certificate.

Certificate	\times
General Details Certification Path	
Certification path angelort-RootCA2 angelort-ad	
View Certificate Certificate status:]
This certificate is OK.	
OK	

17. Repeat steps 10-14 to export the certificate of the root CA which signed the certificate used for LDAPS authentication.

Note: Your deployment can have a multi-tier CA Hierarchy, in which case you need to follow the same procedure to export all the intermediate certificates in the trust chain.

18. Before you continue, ensure that you have one certificate file for the LDAPS server and for each issuer authority in the certification path: Root certificate and intermediate certificates (if applicable).

📙 💆 📑 🗢 LDAPS certificates						- 0	×
File Home Share View							^ 😲
Image: Second system Image: Se	Move Copy to * Copy	New folder New item ▼	Properties	Select all Select none Invert selection			
Clipboard	Organize	New	Open	Select			
← → ヾ ↑ 📔	LDAPS certificates				ע ט Searc	h LDAPS certificates	Q
^ Name	^ D	ate modified Type	Size				
LDAPS_Ro	otCA 11	/25/2021 11:46 Security	y Certificate 3	KB			
LDAPSide	ertificate 11	/24/2021 7:59 PM Security	y Certificate 3	KB			

Step B. Log into the SNA Manager to add the certificate of the LDAP server

and the root chain.

- 1. Navigate to **Central Management** > Inventory.
- 2. Locate the SNA Manager appliance and click **Actions > Edit Appliance Configuration**.
- In the Appliance Configuration window navigate to Configuration Menu > Trust Store > Add New.
- 4. Type the Friendly Name, click **Choose File** and select the certificate of the LDAP Server, then click **Add Certificate**.
- 5. Repeat the previous step to add the Root CA certificate and intermediate certificates (if applicable).
- 6. Verify that the certificates which were uploaded are the correct ones and click **Apply Settings**.

cisco Stealthw	atch Central Mana	gement App	iance Manager	Update Manager	App Manager	Smart Licensing			
Inventory / Appliance Config	Appliance Config Appliance Networ	guration - SMC	0001 2100 PMIN	-				Cancel Apply Settings Configuration Menu V	
	Trust Store Mode	fed						Add New	
	FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS	
	-	-						Delete	
	LDAP-Server	angelort-ad-	angelort-RootCA	2		-		Delete	
	LDAP-server-RootCA	angelort-RootCA2	angelort-RootCA	.2		- 10.00		Delete	
	10 Certificates								
	Revert								

7. Wait for the changes to be applied and for the Manager status to be **Up**.

Step C. Add the LDAP external service configuration.

SNA Version 7.2 or later

1. Open the Manager main dashboard and navigate to **Global Settings** > **User Management**.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure •	Deploy *	۹ 🛓 🗢 ±
			Global Settings
Security Insight Dashboard Inside Hosts			Central Management
			SMC Configuration
Alarming Hosts ()			Packet Analyzer Configuration
		and the second sec	UDP Director Configuration
			External Lookup Configuration
survivore sentines southers		sections and sections in the section of the	User Management
8.4		100	SecureX Configuration
			Select Language

- 2. In the User Management window select the Authentication and Authorization tab.
- 3. Click Create > Authentication Service.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Con	figure • Deploy •		< ⊥ ☆ ±
User Management				
Users Data Roles Authentication and Authorizi	ation			Create
				User
				Data Role
Name	∧ Description	Authentication Type	Remote Authorization	Authentication Service
Ex. local	Filter Authentication Service Description	Ex. LOCAL	~	
	There is no data to	o display		
10 10				
10 enterns per page				

4. From the Authentication Service drop-down menu select LDAP.

5. Complete the required fields.

Field	Notes
Friendly Name	Enter a name for theLDAPserver.
Description	Enter a description for the LDAP server.
	Enter the fully qualified domain name as spec in the Subject Alternative Name (SAN) field of LDAP server certificate.
Server Address	 If the SAN field contains only the IPv4 address enter the IPv4 address in the Server Address If the SAN field contains the DNS name, enter DNS name in the Server Address field. If the SAN field contains both DNS and IPv4 values, use the first value listed. Enter the port designated for secure LDAP
Port	communication (LDAP over TLS). The well known port for LDAPS is 636. Enter the user ID used to connect to the LDAP se For example: CN=admin,OU=Corporate Users,DC=example,DC=com
Bind User	Note : If you have added your users to a buil AD container (For example, "Users"), then th Bind DN of the Bind User must have the canonical name (CN) set to the built-in folde instance, CN=username, CN=Users, DC=domain, DC=com). However, if you hav added your users to a new container, then th Bind DN must have the organizational unit (of set to the new container name (For instance CN=username, OU=Corporate Users, DC=domain, DC=com).
	Note : A useful way to find the Bind DN of the Bind User is to query the Active Directory on Windows Server which has connectivity to th Active Directory Server. To get this information you can open a Windows command prompt

type the command dsquery user dc= <distinguished>,dc=<name> - name <user>. For example: dsquery user dc=example,dc=com -name user1. The resonance looks like "CN=user1,OU=Corporate Users,DC=example,DC=com"</user></name></distinguished>
Enter the Bind User password used to connect to LDAP server. Enter the Distinguished Name (DN). The DN applies to the branch of the directory in w searches for users must begin. It is often the top directory tree (your domain), but you can also spe sub-tree within the directory. The Bind User and t users intended to be authenticated must be access from Base Accounts.

For example: DC=example,DC=com

6. Click Save.

Base Accounts

Password

cisco Stealthwatch Deshboards Monitor Analyze Jobs -	Configure - Deploy - Q 👗 🔅 🕂						
Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.	Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.						
User Management Authentication Service	Cancel						
* = Required							
Friendly Name *	Authentication Service						
angelort LDAP server	LDAP V						
Description *	Port *						
Main AD server	636						
Server Address 🚯 *	Bind User 🚯 *						
angelort-ad-	CN+sOU+SNA,OU+Cisco,DC+zitrosDC+local						
Certificate Revocation 📀 •	Base Accounts 🜒 •						
Disabled V	DC=zitros ,DC=local						
Password *	Confirm Password *						

7. If the settings entered and the certificates added to the trust store are correct, you must get a "You've successfully saved your changes" banner.

8. The configured server must be displayed under **User Management > Authentication and Authorization**.

cisco Stealthwatch	Dashboards •	Monitor *	Analyze *	Jobs *	Configure •	Deploy •			۹ ք	◊ ±
User Management										
Users Data Roles Authentication and Authorization										Create ~
Name	∧ Descript	tion					Authentication Type	Remote Authorization	Actions	
Ex. local	V Filter A	uthentication Se	wice Description				Ex. LOCAL V			
angelort LDAP server	Main AD) server					LDAP			

SNA Version 7.1

- 1. Navigate to **Central Management** > Inventory.
- 2. Locate the SMC appliance and click Actions > Edit Appliance Configuration.
- In the Appliance Configuration window navigate to Configuration Menu > LDAP Setup > Add New.

-

4. Complete the required fields as described in SNA Version 7.2 or later step 5.

cisco electrination contra manegement		
Appliance Configuration - SMC Appliance Network Services General	Cancet Apply Settings Configuration Menu 💌	
LDAP Setup	Add New	
Add LDAP		
FRENDLY NAME * angelort LDAP server	DESCRIPTION * Main AD server	
server ADDRess * angelort-ad-	PORT * 636	
CERTFICATE REVOCATION * Disabled	BIND USER + CN==OU+SNA,OU+Cisco,DC+zitrcDC+local	
PASSWORD *	CONFIRM PASSWORD *	
BASE ACCOUNTS *		
DC=zitro,DC=local		
	Cancel Add	

5. Click Add.

6. Click Apply Settings.

7. Once the settings entered and the certificates added to the trust store are correct, the changes on the Manager are applied and the appliance state must be **Up**.

Step D. Configure Authorization settings.

SNA supports both Local and Remote Authorization via LDAP. With this configuration, the LDAP groups from the AD Server are mapped to built-in or custom SNA roles.

The supported authentication and authorization methods for SNA via LDAP are:

- Remote Authentication & Local Authorization
- Remote Authentication & Remote Authorization (Only supported for SNA version 7.2.1 or later)

Local Authorization

In this case, the users and their roles need to be defined locally. To achieve this, proceed as follows.

- 1. Navigate to User Management again, click the Users tab > Create > User.
- 2. Define the user name to authenticate with the LDAP server and select the configured server

from the Authentication Service drop-down menu.

3. Define the permissions that the user must have over the Manager once it's authenticated by the LDAP server and click **Save**.

Stealthwatch Dashboards • Monitor • J	unalyze • Jobs • Configure • Deploy •	0 1 🔅 🗄
er Management User		Cancel
User Name *	Authentication Service	
user20	angelort LDAP server V	
Full Name	Password 💿	
		Generate Password
Email	Confirm Password	
	Show Password	
Role Settings		
100 0000.30		
Primary Admin		
Data Role		
All Data (Read & Write)		
Web Desktop		
Prob Downey		
Web Roles Compare		
Configuration Manager Analyst Power Analyst		

Remote Authorization via LDAP

Remote Authentication and Authorization via LDAP was first supported in Secure Network Analytics version 7.2.1.

Note: Remote Authorization with LDAP is not supported in version 7.1.

It is relevant to mention that if a user is defined and enabled locally (in the Manager), then the user is authenticated remotely, but authorized locally. The user selection process is as follows:

- 1. Once the credentials are entered on the Manager's welcome page, the Manager looks for a local user with the specified name.
- 2. If a local user is found and it is enabled, it is authenticated remotely (if remote authentication via LDAP with local authorization was configured previously) but authorized with the local settings.
- 3. If remote authorization is configured and enabled, and the user is not found locally (not configured or disabled), both authentication and authorization are performed remotely.

For this reason, the steps to successfully configure remote Authentication are t..

Step D-1. Disable or delete the users intended to use remote authorization but which are defined locally.

- 1. Open the Manager main dashboard and navigate to Global Settings > User Management.
- 2. Disable or delete the users (if they exist) intended to use remote authentication and authorization via LDAP, but are configured locally.

User Management								
Users Data Roles	Authentication and Authorization							Create ~
User Name	Full Name	Primary Admin 🌖	Config Manager 🔵	Analyst 😗	Power Analyst 😑	Data Role	Status	Actions
Ex. jsmith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On	
admin	Admin User	~				All Data (Read & Write)	C On	
angelort	Angel Ortiz	~				All Data (Read & Write)	On	
user20			\checkmark	~		All Data (Read & Write)	Off Off]

Step D-2. Define cisco-stealthwatch Groups in the Microsoft AD server.

For External Authentication and Authorization via LDAP users, passwords and *cisco-stealthwatch* groups are defined remotely in Microsoft Active Directory. The *cisco-stealthwatch* groups to be defined in the AD server are related to the different roles which SNA has, they must be defined as follows.

SNA Role	Group(s) Name
Primary Admin	 cisco-stealthwatch-master-admin cisco-stealthwatch-all-data-read-and-write cisco-stealthwatch-all-data-read-only
Data Role	 cisco-stealthwatch-<custom> (optional)</custom>
	Note: Ensure that custom data role groups b with "cisco-stealthwatch-".
Web Functional Role	 cisco-stealthwatch-configuration-manager cisco-stealthwatch-power-analyst cisco-stealthwatch-analyst cisco-stealthwatch-desktop-stealthwatch-powuser
Desktop Functional Role	 cisco-stealthwatch-desktop-configuration-ma cisco-stealthwatch-desktop-network-engineer cisco-stealthwatch-desktop-security-analyst cisco-stealthwatch-desktop-<custom> (option)</custom>
	Note: Ensure that custom desktop functiona groups begin with "cisco-stealthwatch-deskto

File Action View Help	3 🖸 📑 👔 🐍 📚 🛅 🝸 💆 🍇		
Active Directory Users and C Active Directory Users and C Addmin Addmin Addmin Addmin Addmin Addmin SNA SNA Computers Domain Controllers ForeignSecurityPrinci Managed Service Acc	Name Image: cisco-stealthwatch-all-data-read-and-write Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-all-data-read-only Image: cisco-stealthwatch-configuration-manager Image: cisco-stealthwatch-custom1 Image: cisco-stealthwatch-desktop-custom1 Image: cisco-stealthwatch-desktop-network-engineer Image: cisco-stealthwatch-desktop-security-analyst Image: cisco-stealthwatch-desktop-stealthwatch-power-user Image: cisco-stealthwatch-desktop-stealthwatch-power-user Image: cisco-stealthwatch-master-admin Image: cisco-stealthwatch-power-analyst Image: cisco-stealthwatch-power-analyst	Type Security Group Security Group	Descriptior ^

 \times

Note: As described previously, custom groups are supported for "Data Role" and "Desktop Functional Role" as long as the group name is prepended with the proper string. These custom roles and groups must be defined in both the SNA Manager and the Active Directory server. For example, if you define a custom role "custom1" in the SNA Manager for a desktop client role, it must be mapped to cisco-stealthwatch-desktop-custom1 in Active Directory.

Step D-3. Define LDAP Authorization Group Mappings for the users.

Active Directory Users and Computers

Once the *cisco-stealthwatch* groups have been defined in the AD server, we can map the users intended to have access to the SNA Manager to the necessary groups. This must be done as follows.

• A Primary Admin user must be assigned to the *cisco-stealthwatch-master-admin* group and must not be a member of any other *cisco-stealthwatch* groups.

user20 Properties				? ×
Remote control	COM+			
General Address	Account	Profile	Telephones	Organization
Member Of	Dial-in	Envi	ronment	Sessions
Member of: Name Pri Cisco-stealthwatch-m Domain Users	mary Admin aster-admin		Active Dire zitrosystem zitrosystem	ectory Doma is Jocal/Cisc is Jocal/Use
Add F Primary group: Do	lemove omain Users	o need to c	change Primary o	>
Set Primary Group	you have application	Macintosh 15. ancel	clients or POSIX	-compliant Help

- Each user, other than Primary Admin users, must be assigned to a group of each role with the next conditions.
- 1. Data Role: The user must be assigned to only one group.
- 2. Web Functional Role: The user must be assigned to at least one group.
- 3. Desktop Functional Role: The user must be assigned to at least one group.

snauser10 Properties					?	×	
Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dial-in Environment					COM+ Organization		
Member of:	CHENT	011			00000		
Name cisco-stealthwatch-ci cisco-stealthwatch-ci cisco-stealthwatch-di Data Ro Web Fur Desktop	I data read-an onfiguration m esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu esktop-configu	d-write anager uration-man e Role	ager	Active	Directory	D	
<						>	
Add R	emove					_	
Primary group: Do	main Users There is n you have application	o need to o Macintosh 18.	change Pr clients or	imary gr POSIX-	roup unle compliar	tss t	
OF	((ancel	Арр	ły	H	elp	

Step D-4. Enable Remote Authorization via LDAP on the SNA Manager.

- 1. Open the Manager main dashboard and navigate to **Global Settings** > **User Management**.
- 2. In the User Management window select the Authentication and Authorization tab.
- 3. Locate the LDAP authentication service which was configured in Step C.
- 4. Click Actions > Enable Remote Authorization.

Note: **Only one external Authorization service can be in use at a time.** If another Authorization service is already in use, it is automatically disabled and the new one is enabled, however all users which were authorized with the previous external service are logged out. A confirmation message is displayed before any action takes place.

Use	er Mana	gement					
Us	ers D	ata Roles	Authentication and Authorization				
	Name		^	Description	Authentication Type	Remote Authorization	Actions
	Ex. local		~	Filter Authentication Service Description	Ex. LOCAL ~		
	angelort LD	AP server		Main AD server	LDAP	~	

Verify

The users are able to log in with the credentials defined on the AD server.



The second verification step is in regards to Authorization. In this example, user "user20" was made a member of the *cisco-stealthwatch-master-admin* group in the AD server, and we can confirm that the user has Primary Admin permissions. The user is not defined in the local users, so we can confirm that the Authorization attributes were sent by the AD server.

cisco	Stealthwatch	Dashboards *	Monitor * Analyze	 Jobs Configure 	 Deploy • 			۹	-	¢ ±
User	Management							Online Help	-	
User	Data Roles Authentication and	Authorization						Resources		Create 🗸
	_							Logout		
Use	er Name	Full Name	Primary Admin 😗	Config Manager 🔵	Analyst 😑	Power Analyst 📀	Data Role	Status	Actions	
Ð	. jsmith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On		
adr	nin	Admin User	~				All Data (Read & Write)	💽 On .		
(10 v items per page						1 - 1 of 1 items \parallel \leq	< 1 / 1	> :	

The same verification is done for the other user in this example "snauser10". We can confirm successful authentication with the credentials which were configured on the AD server.



For the Authorization verification, as this user does not belong to the Primary Admin group, some features are not available.

cisco Stealthw	atch	-	Dashboards • N	fonitor * Analyze *	Jobs * Configure	Deploy *				a ք 👸	<u>+</u>
										Global Settings	
Security Insight Da	ashboard Inside H	losts								SMC Configuration	
										Packet Analyzer Configuration	
Alarming Hosts										External Lookup Configuration	1
, assisted a										SecureX Configuration	
Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Poli		
2	0	0	0	0	0	0	0	0		Select Language	

Troubleshoot

If the configuration of the Authentication Service cannot be saved successfully verify that:

- 1. You have added the proper certificates of the LDAP server to the trust store of the Manager.
- 2. The configured Server Address is as specified in the Subject Alternative Name (SAN) field of the LDAP server certificate. If the SAN field contains only the IPv4 address, enter the IPv4 address in the Server Address field. If the SAN field contains the DNS name, enter the DNS name in the Server Address field. If the SAN field contains both DNS and IPv4 values, use the first value listed.
- 3. The configured Bind User and Base Account fields are correct, as specified by the AD

Domain Controller.

Related Information

For additional assistance, please contact Cisco Technical Assistance Center (TAC). A valid support contract is required: <u>Cisco Worldwide Support Contacts.</u>