



Cisco Secure Network Analytics

TACACS+ Configuration Guide 7.5.1



Table of Contents

Introduction	4
Audience	4
Terminology	4
Compatibility	5
Response Management	5
Failover	5
Preparation	6
User Roles Overview	7
Configuring User Names	7
Case-Sensitive User Names	7
Duplicated User Names	7
Earlier Versions	7
Configuring Identity Groups and Users	8
Primary Admin Role	8
Combination of Non-Admin Roles	8
Attribute Values	9
Roles Summary	9
Data Roles	9
Web Roles	10
Desktop Client Roles	10
Process Overview	11
1. Configure TACACS+ in ISE	12
Before you Begin	12
User Names	12
User Roles	12
1. Enable Device Administration in ISE	12
2. Create TACACS+ Profiles	13
Primary Admin Role	15

Combination of Non-Admin Roles	15
3. Map Shell Profiles to Groups or Users	16
4. Add Secure Network Analytics as a Network Device	17
2. Enable TACACS+ Authorization in Secure Network Analytics	18
3. Test Remote TACACS+ User Login	20
Troubleshooting	21
Scenarios	21
Contacting Support	23
Change History	24

Introduction

Terminal Access Controller Access-Control System (TACACS+) is a protocol that supports authentication and authorization services and allows a user to access multiple applications with one set of credentials. Use the following instructions to configure TACACS+ for Cisco Secure Network Analytics (formerly Stealthwatch).

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for installing and configuring Secure Network Analytics products.

If you prefer to work with a professional installer, please contact your local Cisco Partner or contact [Cisco Support](#).

Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics product, including virtual products such as the Cisco Secure Network Analytics Flow Sensor Virtual Edition.

A “**cluster**” is your group of Secure Network Analytics appliances that are managed by the Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console or SMC).



In v7.4.0 we rebranded our Cisco Stealthwatch Enterprise products to Cisco Secure Network Analytics. For a complete list, refer to the [Release Notes](#). In this guide, you will see our former product name, Stealthwatch, used whenever necessary to maintain clarity, as well as terminology such as Stealthwatch Management Console and SMC.

Compatibility

For TACACS+ authentication and authorization, make sure all users log in through the Manager. To log in to an appliance directly and use the Appliance Administration, log in locally.

The following features are not available when TACACS+ is enabled: FIPS, Compliance Mode.

Response Management

Response Management is configured in your Manager. To receive email alerts, scheduled reports, etc. make sure the user is configured as a local user on the Manager. Go to **Configure > Detection > Response Management**, and refer to the Help for instructions.

Failover

Please note the following information if you've configured your Managers as a failover pair:

- TACACS+ is only available on the primary Manager. TACACS+ is not supported on the secondary Manager.
- If TACACS+ is configured on the primary Manager, the TACACS+ user information is not available on the secondary Manager. Before you can use configured external authentication services on a secondary Manager, you need to promote the secondary Manager to primary.
- If you promote the secondary Manager to primary:
 - Enable TACACS+ and remote authorization on the secondary Manager.
 - Any external users logged into the demoted primary Manager will be logged out.
 - The secondary Manager does not retain user data from the primary Manager, so any data saved on the primary Manager is not available on the new (promoted) primary Manager.
 - Once the remote user logs in to the new primary Manager for the first time, the user directories will be created and the data is saved going forward.
- **Review Failover Instructions:** For more information, refer to the [Failover Configuration Guide](#).

Preparation

You can configure TACACS+ on Cisco Identity Services Engine (ISE). Make sure you have everything you need to start the configuration.

Requirement	Details
Cisco Identity Services Engine (ISE)	Install and configure ISE using the instructions in the ISE documentation for your engine . You will need the IP address, port, and shared secret key for the configuration. You will also need the Device Administration license.
TACACS+ Server	You will need the IP address, port, and shared secret key for the configuration.
Desktop Client	You will use the Desktop Client for this configuration. To install the Desktop Client, refer to the Cisco Secure Network Analytics System Configuration Guide that matches your Secure Network Analytics version.

User Roles Overview

This guide includes instructions for configuring your TACACS+ users for remote authentication and authorization. Before you start the configuration, review the details in this section to ensure you configure your users correctly.

Configuring User Names

For remote authentication and authorization, you can configure your users in ISE. For local authentication and authorization, configure your users in the Manager.

- **Remote:** To configure your users in ISE, follow the instructions in this configuration guide.
- **Local:** To configure your users locally only, log in to the Manager. From the main menu, select **Configure > Global > User Management**. Select Help for instructions.

Case-Sensitive User Names

When you configure remote users, enable case-sensitivity on the remote server. If you do not enable case-sensitivity on the remote server, users may not be able to access their data when they log in to Secure Network Analytics.

Duplicated User Names

Whether you configure user names remotely (in ISE) or locally (in the Manager), make sure all user names are unique. We do not recommend duplicating user names across remote servers and Secure Network Analytics.

If a user logs in to the Manager, and they have the same user name configured in Secure Network Analytics and ISE, they will only access their local Manager/Secure Network Analytics data. They cannot access their remote TACACS+ data if their user name is duplicated.

Earlier Versions

If you've configured TACACS+ in an earlier version of Cisco Secure Network Analytics (Stealthwatch v7.1.1 and earlier), make sure you create new users with unique names for v7.1.2 and later. We do not recommend using or duplicating the user names from earlier versions of Secure Network Analytics.

To continue using user names that were created in v7.1.1 and earlier, we recommend changing them to **local** only in your primary Manager and the Desktop Client. Refer to the Help for instructions.

Configuring Identity Groups and Users

For an authorized user login, you will map shell profiles to your users. For each shell profile, you can assign the [Primary Admin](#) role or create a [combination of non-admin roles](#). If you assign the Primary Admin role to a shell profile, no additional roles are permitted. If you create a combination of non-admin roles, make sure it meets the requirements.

Primary Admin Role

Primary Admin can view all functionality and change anything. If you assign the Primary Admin role to a shell profile, no additional roles are permitted.

Role	Attribute Value
Primary Admin	cisco-stealthwatch-master-admin

Combination of Non-Admin Roles

If you create a combination of non-admin roles for your shell profile, make sure it includes the following:

- 1 Data role (only)
- 1 or more Web role
- 1 or more Desktop Client role

For details, refer to the [Attribute Values](#) table.



If you assign the Primary Admin role to a shell profile, no additional roles are permitted. If you create a combination of non-admin roles, make sure it meets the requirements.

Attribute Values

For more information about each type of role, click the link in the Required Roles column.

Required Roles	Attribute Value
1 Data role (only)	<ul style="list-style-type: none"> cisco-stealthwatch-all-data-read-and-write cisco-stealthwatch-all-data-read-only
1 or more Web role	<ul style="list-style-type: none"> cisco-stealthwatch-configuration-manager cisco-stealthwatch-power-analyst cisco-stealthwatch-analyst
1 or more Desktop Client role	<ul style="list-style-type: none"> cisco-stealthwatch-desktop-stealthwatch-power-user cisco-stealthwatch-desktop-configuration-manager cisco-stealthwatch-desktop-network-engineer cisco-stealthwatch-desktop-security-analyst

Roles Summary

We've provided a summary of each role in the following tables. For more information about user roles in Secure Network Analytics, review the User Management page in Help.

Data Roles

Make sure you choose only one data role.

Data Role	Permissions
All Data (Read Only)	The user can view data in any domain or host group, or on any appliance or device, but cannot make any configurations.
All Data (Read & Write)	The user can view and configure data in any domain or host group, or on any appliance or device.

The specific functionality (flow search, policy management, network classification, etc.) that the user can view and/or configure is determined by the user's web role.

Web Roles

Web Role	Permissions
Power Analyst	The Power Analyst can perform the initial investigation into traffic and flows as well as configure policies and host groups.
Configuration Manager	The Configuration Manager can view configuration-related functionality.
Analyst	The Analyst can perform the initial investigation into traffic and flows.

Desktop Client Roles

Web Role	Permissions
Configuration Manager	The Configuration Manager can view all menu items and configure all appliances, devices, and domain settings.
Network Engineer	The Network Engineer can view all traffic-related menu items within the Desktop Client, append alarm and host notes, and perform all alarm actions, except mitigation.
Security Analyst	The Security Analyst can view all security-related menu items, append alarm and host notes, and perform all alarm actions, including mitigation.
Stealthwatch (Secure Network Analytics) Power User	The Stealthwatch (Secure Network Analytics) Power User can view all menu items, acknowledge alarms, and append alarm and host notes, but without the ability to change anything.

Process Overview

You can configure Cisco ISE to provide TACACS+. To successfully configure TACACS+ settings and authorize TACACS+ in Secure Network Analytics, make sure you complete the following procedures:

- 1. Configure TACACS+ in ISE**
- 2. Enable TACACS+ Authorization in Secure Network Analytics**
- 3. Test Remote TACACS+ User Login**

1. Configure TACACS+ in ISE

Use the following instructions to configure TACACS+ on ISE. This configuration enables your remote TACACS+ users on ISE to log in to Secure Network Analytics.

Before you Begin

Before you start these instructions, install and configure ISE using the instructions in the [ISE documentation for your engine](#). This includes making sure your certificates are set up correctly.

User Names

Whether you configure user names remotely (in ISE) or locally (in the Manager), make sure all user names are unique. We do not recommend duplicating user names across remote servers and Secure Network Analytics.

Duplicated User Names: If a user logs in to the Manager, and they have the same user name configured in Secure Network Analytics and ISE, they will only access their local Manager/Secure Network Analytics data. They cannot access their remote TACACS+ data if their user name is duplicated.

Case-Sensitive User Names: When you configure remote users, enable case-sensitivity on the remote server. If you do not enable case-sensitivity on the remote server, users may not be able to access their data when they log in to Secure Network Analytics.

User Roles

For each TACACS+ profile in ISE, you can assign the [Primary Admin](#) role or create a [combination of non-admin roles](#).

If you assign the Primary Admin role to a shell profile, no additional roles are permitted. If you create a combination of non-admin roles, make sure it meets the requirements. For more information about user roles, refer to [User Roles Overview](#).

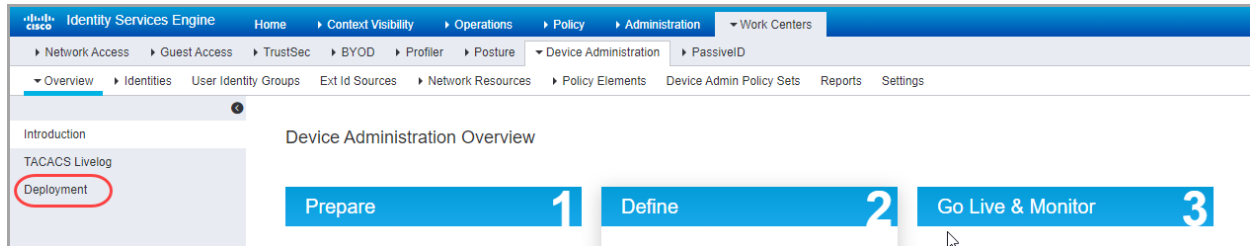
1. Enable Device Administration in ISE

Use the following instructions to add the TACACS+ service to ISE.

1. Log in to your ISE as an admin.
2. Select **Work Centers > Device Administration > Overview**.

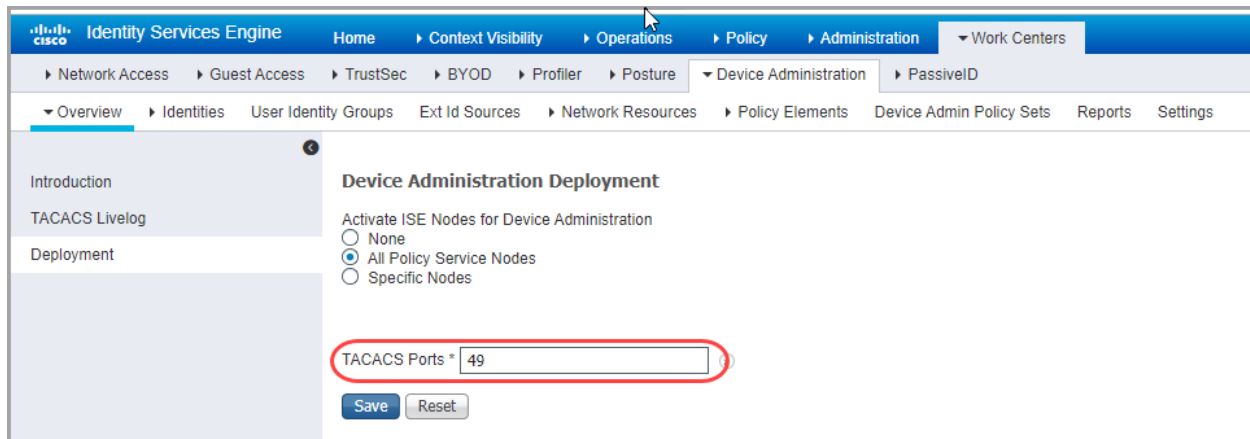
If Device Administration is not shown in Work Centers, go to **Administration > System > Licensing**. In the Licensing section, confirm the Device Administration License is shown. If it is not shown, add the license to your account.

3. Select **Deployment**.



4. Select **All Policy Service Nodes** or **Specific Nodes**.

5. In the TACACS Ports field, enter **49**.



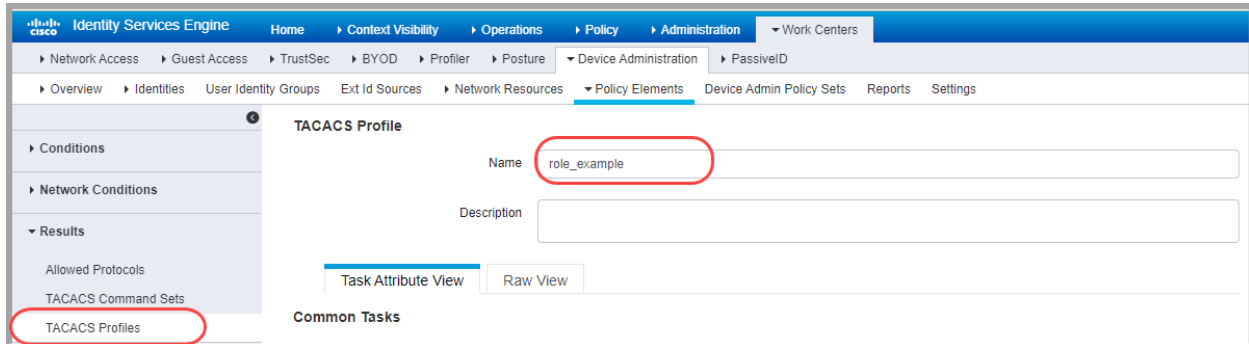
6. Click **Save**.

2. Create TACACS+ Profiles


Use the following instructions to add TACACS+ shell profiles to ISE. You will also use these instructions to assign the required roles to the shell profile.

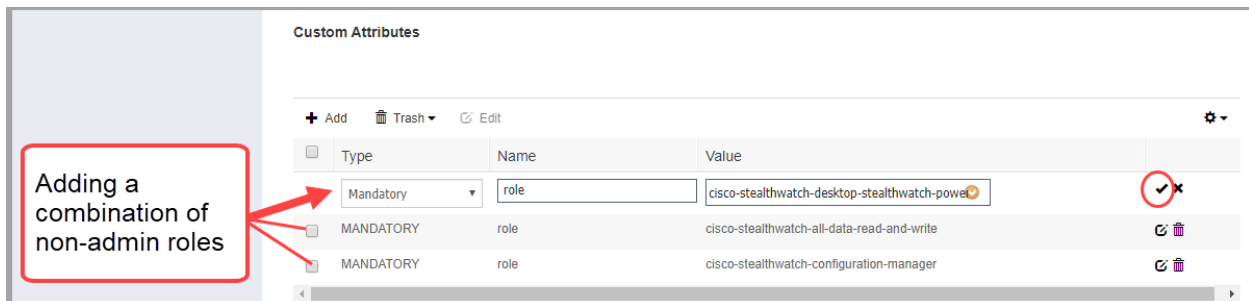
1. Select **Work Centers > Device Administration > Policy Elements**.
2. Select **Results > TACACS Profiles**.
3. Click **+Add**.
4. In the Name field, enter a unique user name.

For details about user names refer to [User Roles Overview](#).



5. In the Common Task Type drop-down, select **Shell**.
6. In the Custom Attributes section, click **+Add**.
7. In the Type field, select **Mandatory**.
8. In the Name field, enter **role**.
9. In the Value field, enter the attribute value for [Primary Admin](#) or build a [combination of non-admin roles](#).

- **Save:** Click the  Check icon to save the role.
- **Combination of Non-Admin Roles:** If you create a combination of non-admin roles, repeat steps 5 through 8 until you have added a row for each required role (Data role, Web role, and Desktop Client role).



Primary Admin Role

Primary Admin can view all functionality and change anything. If you assign the Primary Admin role to a shell profile, no additional roles are permitted.

Role	Attribute Value
Primary Admin	cisco-stealthwatch-master-admin

Combination of Non-Admin Roles

If you create a combination of non-admin roles for your shell profile, make sure it includes the following:

- 1 Data role (only): make sure you select only one data role
- 1 or more Web role
- 1 or more Desktop Client role

Required Roles	Attribute Value
1 Data role (only)	<ul style="list-style-type: none"> • cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only
1 or more Web role	<ul style="list-style-type: none"> • cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
1 or more Desktop Client role	<ul style="list-style-type: none"> • cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineer • cisco-stealthwatch-desktop-security-analyst



If you assign the Primary Admin role to a shell profile, no additional roles are permitted. If you create a combination of non-admin roles, make sure it meets the requirements.

10. Click **Save**.
11. Repeat the steps in **2. Create TACACS+ Profiles** to add any additional TACACS+ shell profiles to ISE.

3. Map Shell Profiles to Groups or Users

Use the following instructions to map your shell profiles to your authorization rules.

1. Select **Work Centers > Device Administration > Device Admin Policy Sets**.
2. Locate your policy set name. Click the **➤** Arrow icon.
3. Locate your authorization policy. Click the **➤** Arrow icon.
4. Click the **+** Plus icon.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets. The main content area is titled 'Policy Sets' and contains a table with the following columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is located above the table. The table shows one policy set with a status of 'OK' and a name of 'Default'. Below the table, there is a section for 'Authentication Policy (1)' with a search bar and a plus icon. A red circle highlights the plus icon in this section. Below the plus icon, there is a section for 'Authorization Policy - Local Exceptions' and 'Authorization Policy - Global Exceptions'.

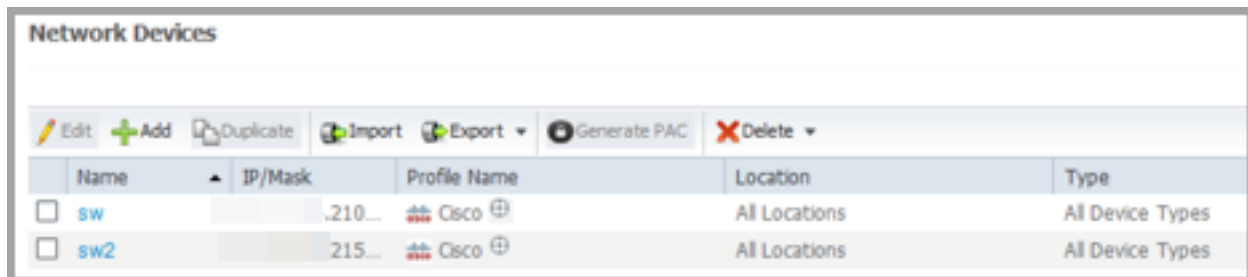
5. In the Conditions field, click the **+** Plus icon. Configure the policy conditions.

Help: For Conditions Studio instructions, click the **?** Help icon.

6. In the Shell Profiles field, select the shell profile you created in **2. Create TACACS+ Profiles**.
7. Repeat the steps in **3. Map Shell Profiles to Groups or Users** until you have mapped all shell profiles to your authorization rules.

4. Add Secure Network Analytics as a Network Device

1. Select **Administration > Network Resources > Network Devices**.
2. Select Network Devices, click **+Add**.
3. Complete the information for your primary Manager, including the following fields:
 - **Name:** Enter the name of your Manager.
 - **IP Address:** Enter the Manager IP address.
 - **Shared Secret:** Enter the shared secret key.
4. Click **Save**.
5. Confirm the network device is saved to the Network Devices list.



Network Devices					
Edit +Add Duplicate Import Export Generate PAC Delete					
Name	IP/Mask	Profile Name	Location	Type	
<input type="checkbox"/> sw	.210...	Cisco	All Locations	All Device Types	
<input type="checkbox"/> sw2	215...	Cisco	All Locations	All Device Types	

6. Go to [2. Enable TACACS+ Authorization in Secure Network Analytics](#).

2. Enable TACACS+ Authorization in Secure Network Analytics

Use the following instructions to add the TACACS+ server to Secure Network Analytics and enable remote authorization.



Only a Primary Admin can add the TACACS+ server to Secure Network Analytics.

1. Log in to your primary Manager.
2. From the main menu, select **Configure > Global > User Management**.
3. Click the **Authentication and Authorization** tab.
4. Click **Create**. Select **Authentication Service**.
5. Click the Authentication Service drop-down. Select **TACACS+**.
6. Complete the fields:

Field	Notes
Name	Enter a unique name to identify the server.
Description	Enter a description which specifies how or why the server is being used.
Cache Timeout (Seconds)	The amount of time (in seconds) that a user name or password is considered valid before Secure Network Analytics requires re-entry of the information.
Prefix	This field is optional. The prefix string is placed at the beginning of the user name when the name is sent to the RADIUS or TACACS+ server. For example, if the user name is zoe and the realm prefix is <i>DOMAIN-A\</i> , the user name DOMAIN-A\zoe is sent to the server. If you do not configure the Prefix field, only the user name is sent to the server.

Suffix	This field is optional. The suffix string is placed at end of the user name. For example, if the suffix is <i>@mydomain.com</i> , the username <i>zoe@mydomain.com</i> is sent to the TACACS+ server. If you do not configure the Suffix field, only the user name is sent to the server.
--------	---

7. In the Servers section, click **Add New**.
8. Complete the following fields.

Field	Notes
IP Address	Use either IPv4 or IPv6 addresses when configuring authentication services.
Port	Enter any numbers from 0 to 65535 which correspond to the applicable port.
Secret Key	Enter the secret key that was configured for the applicable server.

9. Click **Add**.
10. Click **Save**.
11. Confirm the new TACACS+ server is shown in the list.
12. Click the **Actions** menu for the TACACS+ server.
13. Select **Enable Remote Authorization** from the drop-down menu.
14. Follow the on-screen prompts to enable TACACS+.

3. Test Remote TACACS+ User Login

Use the following instructions to log in to the Manager. For remote TACACS+ authorization, make sure all users log in through the Manager.



To log in to an appliance directly and use the Appliance Administration, log in locally.

1. In the address field of your browser, type the following:

https:// followed by the IP address of your Manager.

2. Enter the user name and password of a remote TACACS+ user.
3. Click **Sign In**.

If a user cannot log in to the Manager, review the Troubleshooting section.

Troubleshooting

If you encounter any of these troubleshooting scenarios, contact your administrator to review the configuration with the solutions we've provided here. If your admin cannot resolve the issues, please contact [Cisco Support](#).

Scenarios

Scenario	Notes
<p>A specific TACACS+ user cannot log in</p>	<ul style="list-style-type: none"> Review the Audit Log for user login failure with Illegal Mappings or Invalid Combination of Roles. This can happen if the identity group shell profile includes Primary Admin and additional roles, or if the combination of non-admin roles does not meet the requirements. Refer to User Roles Overview for details. Make sure the TACACS+ user name is not the same as a local (Secure Network Analytics) user name. Refer to User Roles Overview for details.
<p>All TACACS+ users cannot log in</p>	<ul style="list-style-type: none"> Check the TACACS+ configuration in Secure Network Analytics. Check the configuration on the TACACS+ server. Make sure the TACACS+ server is running. Make sure the TACACS+ service is enabled in Secure Network Analytics: <ul style="list-style-type: none"> There can be multiple authentication servers defined, but only one can be enabled for authorization. Refer to 2. Enable TACACS+ Authorization in Secure Network Analytics for details. To enable authorization for a specific TACACS+ server, refer to 2. Enable TACACS+ Authorization in Secure Network Analytics for details.

When a user logs in, they can only access the Manager locally

If a user exists with the same user name in Secure Network Analytics (local) and the TACACS+ server (remote), the local login overrides the remote login. Refer to [User Roles Overview](#) for details.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	July 24, 2024	Initial version.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

