# Table of Contents

**Introduction** ................................................................................................................. 4
  - Audience .................................................................................................................. 4
  - Terminology .............................................................................................................. 4
  - Compatibility ............................................................................................................. 4
**Preparation** .................................................................................................................. 5
**User Roles Overview** ..................................................................................................... 6
  - Configuring User Names .......................................................................................... 6
  - Duplicate User Names .............................................................................................. 6
  - Earlier Versions .......................................................................................................... 6
  - Configuring Identity Groups and Users ..................................................................... 6
  - Master Admin Role ..................................................................................................... 7
  - Combination of Non-Admin Roles ........................................................................... 7
  - Attribute Values ........................................................................................................ 8
  - Roles Summary .......................................................................................................... 8
    - Data Roles ............................................................................................................... 8
    - Web Roles ............................................................................................................... 9
    - Desktop Client Roles ............................................................................................. 9
**Process Overview** .......................................................................................................... 10
  **1a. Configuring TACACS+ in ACS** ............................................................................ 11
    - Service Name ......................................................................................................... 11
    1. Add the Device Type ............................................................................................ 11
    2. Add the TACACS+ Server .................................................................................. 13
    3. Authorize the TACACS+ Service ........................................................................ 14
    4. Add Identity Groups to the ACS Server ............................................................. 17
      - Identity Group Name .......................................................................................... 17
      - User Roles ........................................................................................................... 17
      1. Create a New Identity Group .......................................................................... 18
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 Stealthwatch.

Audience

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

If you prefer to work with a professional installer, please contact your local Cisco Partner or Cisco Stealthwatch Support.

Terminology

This guide uses the term “appliance” for any Stealthwatch product, including virtual products such as the Stealthwatch Flow Sensor Virtual Edition (VE).

A "cluster" is your group of Stealthwatch appliances that are managed by the Stealthwatch Management Console (SMC).

Most appliances are managed by the SMC. If an appliance is not managed by the SMC, such as an Endpoint Concentrator, it is described as a "stand-alone appliance."

Compatibility

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

Response Management is configured on the Stealthwatch Desktop Client. To receive email alerts, scheduled reports, etc. make sure the user is configured as a local user on the Stealthwatch Management Console (SMC).

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

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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Secure Access Control System (ACS)</strong> or</td>
<td><strong>ACS</strong>: Install the Cisco Secure ACS server using the instructions in</td>
</tr>
<tr>
<td><strong>Cisco Identity Services (ISE)</strong></td>
<td>the Installation and Upgrade Guide for your model.</td>
</tr>
<tr>
<td></td>
<td><strong>ISE</strong>: Configure ISE using the instructions in the ISE Configuration</td>
</tr>
<tr>
<td></td>
<td>Guide. You will also need the Device Administration license.</td>
</tr>
<tr>
<td>TACACS+ Server</td>
<td>You will need the IP address, port, and shared secret key for the</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td>Microsoft Internet Explorer 11 (ACS only)</td>
<td>If you’re configuring TACACS+ on Cisco Secure Access Control System, use</td>
</tr>
<tr>
<td></td>
<td>this browser.</td>
</tr>
<tr>
<td>Stealthwatch Desktop Client</td>
<td>You will use the Stealthwatch Desktop Client for this configuration. To</td>
</tr>
<tr>
<td></td>
<td>install the Desktop Client, refer to the Stealthwatch Installation and</td>
</tr>
<tr>
<td></td>
<td>Configuration Guide.</td>
</tr>
</tbody>
</table>
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 ACS or ISE. For local authentication and authorization, configure your users in the Stealthwatch Management Console.

- **Remote:** To configure your users in Cisco Secure ACS or Cisco ISE, follow the instructions in this configuration guide.
- **Local:** To configure your users locally only, log in to the SMC. Click the **Global Settings** icon > **User Management**. Select Stealthwatch Online Help for instructions.

Duplicate User Names

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

If a user logs in to the SMC, and they have the same user name configured in Stealthwatch and ACS or ISE, they will only access their local SMC/Stealthwatch 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 Stealthwatch (v7.1.1 or earlier), make sure you create new users with unique names for Stealthwatch v7.1.2. We do not recommend using or duplicating the user names from earlier versions of Stealthwatch.

To continue using user names that were created in v7.1.1 or earlier, we recommend changing them to **local** only in the Stealthwatch Web App (your primary SMC) and the Stealthwatch Desktop Client. Refer to Stealthwatch Online 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 **Master Admin** role or create a **combination of non-admin roles**. If you assign the Master 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.
Master Admin Role

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Admin</td>
<td>cisco-stealthwatch-master-admin</td>
</tr>
</tbody>
</table>

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 Master 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.

<table>
<thead>
<tr>
<th>Required Roles</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Data role (only)</td>
<td>• cisco-stealthwatch-all-data-read-and-write</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-all-data-read-only</td>
</tr>
<tr>
<td>1 or more Web role</td>
<td>• cisco-stealthwatch-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-power-analyst</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-analyst</td>
</tr>
<tr>
<td>1 or more Desktop Client role</td>
<td>• cisco-stealthwatch-desktop-stealthwatch-power-user</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-network-engineer</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-security-analyst</td>
</tr>
</tbody>
</table>

Roles Summary

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

Data Roles

Make sure you choose only one data role.

<table>
<thead>
<tr>
<th>Data Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Data (Read Only)</td>
<td>The user can view data in any domain or host group, or on any appliance or device, but cannot make any configurations.</td>
</tr>
<tr>
<td>All Data (Read &amp; Write)</td>
<td>The user can view and configure data in any domain or host group, or on any appliance or device.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Web Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Analyst</td>
<td>The Power Analyst can perform the initial investigation into traffic and flows as well as configure policies and host groups.</td>
</tr>
<tr>
<td>Configuration Manager</td>
<td>The Configuration Manager can view configuration-related functionality.</td>
</tr>
<tr>
<td>Analyst</td>
<td>The Analyst can perform the initial investigation into traffic and flows.</td>
</tr>
</tbody>
</table>

### Desktop Client Roles

<table>
<thead>
<tr>
<th>Web Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Manager</td>
<td>The Configuration Manager can view all menu items and configure all appliances, devices, and domain settings.</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>The Network Engineer can view all traffic-related menu items within the Stealthwatch Desktop Client, append alarm and host notes, and perform all alarm actions, except mitigation.</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>The Security Analyst can view all security-related menu items, append alarm and host notes, and perform all alarm actions, including mitigation.</td>
</tr>
<tr>
<td>Stealthwatch Power User</td>
<td>The Stealthwatch Power User can view all menu items, acknowledge alarms, and append alarm and host notes, but without the ability to change anything.</td>
</tr>
</tbody>
</table>
Process Overview

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

1. Configure TACACS+ in ACS or ISE.
2. Add the TACACS+ Server to Stealthwatch.
4. Test TACACS+ Login.
1a. Configuring TACACS+ in ACS

Use the following instructions to add the TACACS+ service to Cisco Secure ACS.

To configure TACACS+ on ISE, refer to 1b. Configuring TACACS+ in ISE.

Service Name

When you create a new service name, make sure you record the name because you will enter it in other procedures.

1. Add the Device Type

1. Open Microsoft Internet Explorer 11.
2. Log in to the Cisco Secure ACS.
3. Select the Network Resources menu.
4. Under Network Device Groups, select Device Type.
5. Click Create.
6. In the Name field, enter **Stealthwatch**.

   **This is your TACACS+ service name.** You will use this name to enable TACACS+ in a later procedure. If you enter a different name in this field, make sure you record it.

7. Click **Submit**.
2. Add the TACACS+ Server

1. Select the **Network Devices and AAA Clients** menu.
2. Click **Create**.
3. In the **Name** field, enter **Stealthwatch**.

   Use the same name you entered in **1. Add the Device Type**.

4. In the Location field, select **All Locations**.
5. In the Device Type field, click **Select**.
   - Click the arrow next to All Device Types.
   - Select **Stealthwatch** (or the name you created).
   - Click **OK**.

6. In the IP Address section, select **Single IP Address**.
7. In the IP field, enter your TACACS+ server IP address.
8. In the Authentication Options section, check the **TACACS+** check box.
9. In the Shared Secret field, enter the server password.

10. Click **Submit**.
3. Authorize the TACACS+ Service

Use the following instructions to authorize the TACACS+ service in the Cisco Secure ACS.

1. Select the **Access Policies** menu.
2. Select the **Access Services** menu.
3. Click **Create**.
4. In the Name field, enter **Stealthwatch** (or the **TACACS+ service name** you entered in the previous procedure).

![Image of Cisco Secure ACS interface]

5. Under Access Service Policy Structure, select **Based on service template**. Click **Select** to choose your service policy.
6. Click **Next**.
7. Select protocols or use the default values.
8. Click **Finish**.
9. When prompted, click **Yes** to modify the Service Selection policy to activate the service.

   The following menu opens: Access Policies > Access Services > Service Selection Rules.

10. Click **Create**.
11. In the Name field, enter **Stealthwatch** (service name).
12. In the Status field, select **Enabled**.
13. Check the **Compound Condition** check box.

![Configuration screen](image)

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

14. In the Dictionary field, select **NDG**.
15. In the Attribute field, select **Device Type**.
16. In the Operator field, select **in**.
17. In the Value field, select **Static**.
18. In the blank field under Value, click **Select**.
19. Click the arrow next to All Device Types.
20. Select **Stealthwatch**.
21. Click **OK**.
22. Click **Add**.
23. In the Service field, select **Stealthwatch**.
24. Click **OK**.
4. Add Identity Groups to the ACS Server

Use the following instructions to configure identity groups. For each identity group, you will create a shell profile and authorization access.

Identity Group Name

When you create a new group and name it, make sure you use the same name for the corresponding shell profile and authorization access.

User Roles

For each shell profile, you can assign the Master Admin role or create a combination of non-admin roles.

If you assign the Master 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. Create a New Identity Group

Use the following instructions to create a new identity group.

1. Select the **Users and Identity Stores** menu.
2. Select **Identity Groups**.
3. Click **Create**.

4. In the **Name** field, enter a group name.

   Make sure you use the same name for the corresponding shell profile and authorization access in the later procedures.
5. Click **Submit**.

2. Create a Shell Profile

Use the following instructions to create a shell profile for the identity group you created in the last procedure. You will also use these instructions to assign the required roles to the shell profile.

1. Select the **Policy Elements** menu.
2. Under Authorization and Permissions > Device Administration, select **Shell Profiles**.
3. Click **Create**.
4. In the Name field, enter the Identity Group Name you created in 1. **Create a New Identity Group**.
5. Select the **Custom Attributes** tab.
6. Complete the following fields:
   - Attribute: role
   - Requirement: Mandatory
   - Attribute Value: Static
7. In the blank field under **Attribute Value**, enter the value for **Master Admin** or build a **combination of non-admin roles**.

If you assign the Master 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.

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Admin</td>
<td>cisco-stealthwatch-master-admin</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Role</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Data role (only)</strong></td>
<td>- cisco-stealthwatch-all-data-read-and-write</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-all-data-read-only</td>
</tr>
<tr>
<td><strong>1 or more Web role</strong></td>
<td>- cisco-stealthwatch-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-power-analyst</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-analyst</td>
</tr>
<tr>
<td><strong>1 or more Desktop Client role</strong></td>
<td>- cisco-stealthwatch-desktop-stealthwatch-power-user</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-desktop-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-desktop-network-engineer</td>
</tr>
<tr>
<td></td>
<td>- cisco-stealthwatch-desktop-security-analyst</td>
</tr>
</tbody>
</table>

If you assign the Master 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.
8. Click **Add**.
9. Repeat steps 6 through 8 until you have added **all required roles** to the shell profile.
10. Click **Submit**.

### 3. Configure Identity Group Based Authorization

1. Select the **Access Policies** menu.
2. Select **Access Services > Stealthwatch** (or your service name) > **Authorization**.
3. Click **Create**.
4. In the Name field, enter the Identity Group Name you created in **1. Create a New Identity Group**.
5. In the Status field, select **Enabled**.
6. Check the **Identity Group** check box.
7. Click **Select**.
8. Click the arrow next to All Groups.
9. Select the identity group name from the list.
10. Click **OK**.
11. In the Shell Profile field, click **Select**.
12. Select the identity group name from the list.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Stealthwatch Analyst RO</td>
</tr>
</tbody>
</table>

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

<table>
<thead>
<tr>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Identity Group: in All Groups: Stealthwatch Analyst RO</td>
</tr>
<tr>
<td>❌ NDG Location: ANY-</td>
</tr>
<tr>
<td>❌ NDG Device Type: ANY-</td>
</tr>
<tr>
<td>❌ Time And Date: ANY-</td>
</tr>
<tr>
<td>❌ System: UserName: ANY-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shell Profile: Stealthwatch Analyst RO</td>
</tr>
</tbody>
</table>
13. Click OK.

14. Repeat the instructions in section 4. Add Identity Groups to the ACS Server to create another identity group, configure the shell profile, and assign authorization.

5. Assign Identity Groups to Users

After you’ve configured your Stealthwatch identity groups, assign a group to your Stealthwatch users.

User Names

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

Duplicate User Names: If a user logs in to the SMC, and they have the same user name configured in Stealthwatch and ACS or ISE, they will only access their local SMC/Stealthwatch data. They cannot access their remote TACACS+ data if their user name is duplicated.

Assign Identity Groups to Users

1. Select the Users and Identity Stores menu.
2. Under Internal Identity Stores, select Users.
3. Select a user name from the list, or click Create to configure a new user.
4. In the Identity Group field, click Select.
5. Click the arrow next to All Groups.

6. Select the identity group name.

7. Click OK.

8. Finish the user configuration. Click Submit to save your changes.

9. Repeat the steps in 5. Assign Identity Groups to Users as needed. Then, go to 2. Add the TACACS+ Server to Stealthwatch.
1b. Configuring TACACS+ in ISE

Use the following instructions to configure TACACS+ on Cisco Identity Services Engine (ISE). This configuration enables your remote TACACS+ users on ISE to log in to Stealthwatch.

To configure TACACS+ on ACS, refer to 1a. Configuring TACACS+ in ACS.

Before you Begin

Before you start these instructions, configure ISE using the instructions in the ISE Configuration Guide. This includes making sure your certificates are set up correctly.

User Names

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

Duplicate User Names: If a user logs in to the SMC, and they have the same user name configured in Stealthwatch and ACS or ISE, they will only access their local SMC/Stealthwatch data. They cannot access their remote TACACS+ data if their user name is duplicated.

User Roles

For each TACACS+ profile in ISE, you can assign the Master Admin role or create a combination of non-admin roles.

If you assign the Master 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. Add the TACACS+ Service to Cisco ISE

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

1. Log in to your Identity Services Engine 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 **Master 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).

---

**Master Admin Role**

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Admin</td>
<td>cisco-stealthwatch-master-admin</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Required Roles</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Data role (only)</strong></td>
<td>• cisco-stealthwatch-all-data-read-and-write</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-all-data-read-only</td>
</tr>
<tr>
<td><strong>1 or more Web role</strong></td>
<td>• cisco-stealthwatch-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-power-analyst</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-analyst</td>
</tr>
<tr>
<td><strong>1 or more Desktop Client role</strong></td>
<td>• cisco-stealthwatch-desktop-stealthwatch-power-user</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-configuration-manager</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-network-engineer</td>
</tr>
<tr>
<td></td>
<td>• cisco-stealthwatch-desktop-security-analyst</td>
</tr>
</tbody>
</table>

If you assign the Master 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 **Stealthwatch** (or the name of your preferred policy set). Click the **Arrow icon**.
3. Locate your authorization policy. Click the ➤ Arrow icon.
4. Click the + Plus icon.

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. Then, go to 2. Add the TACACS+ Server to Stealthwatch.
2. Add the TACACS+ Server to Stealthwatch

1. Open the Stealthwatch Desktop Client.
2. Log in as admin.
3. From the Main Menu, select Configuration > User Management.
4. Select Authentication Service.
5. Click Add.
6. Select the TACACS+ authentication service type.
7. Click OK.
8. In the Name field, enter Stealthwatch (or the service name you configured in ACS or ISE).
9. Complete the fields in the dialog box as needed.
10. Click Add.
11. In the **Add TACACS+ Server** dialog box, enter the following information for the TACACS+ server:

   - IP address
   - Port
   - Key

12. Click **OK**.
13. Confirm your TACACS+ service is shown in the Authentication Service list.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Authentication Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch</td>
<td></td>
<td>TACACS+</td>
</tr>
</tbody>
</table>
```
3. Enable TACACS+ Authorization in Stealthwatch

Use the following instructions to enable TACACS+ authorization in Stealthwatch.

If another authorization service is running, disable it before you enable TACACS+.

1. SSH in to the Stealthwatch Management Console (SMC).
2. Log in as root.
3. Type the following command:

   Authorizer.py -e Stealthwatch

In this command, Stealthwatch is the TACACS+ service name you configured in ACS or ISE.

4. Press enter to run the command and enable TACACS+ authorization in Stealthwatch.
4. Test Remote TACACS+ User Login

Use the following instructions to log in to the Stealthwatch Management Console (SMC). For remote TACACS+ authorization, make sure all users log in through the SMC.

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 SMC.

2. Enter the user name and password of a remote TACACS+ user.

3. Click Sign In.

   If a user cannot log in to the SMC, review Troubleshooting.
Disabling Authorization

Use the following instructions to disable TACACS+ authorization in Stealthwatch.

1. SSH in to the Stealthwatch Management Console (SMC).
2. Log in as root.
3. Type the following command:

   Authorizer.py -d Stealthwatch

   In this command, **Stealthwatch** is the TACACS+ service name you configured in ACS or ISE.

4. Press enter to run the command and disable TACACS+ authorization in Stealthwatch.
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 Stealthwatch Support.

Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Notes</th>
</tr>
</thead>
</table>
| A specific TACACS+ user cannot log in | - 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 Master 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 (Stealthwatch) user name. Refer to **User Roles Overview** for details. |
| All TACACS+ users cannot log in | - Check the TACACS+ configuration in Stealthwatch.  
- Check the configuration on the TACACS+ server.  
- Make sure the TACACS+ server is running.  
- Make sure the TACACS+ service is enabled in Stealthwatch:  
  - There can be multiple authentication servers defined, but only one can be enabled for authorization.  
  - To verify which server is currently enabled in Stealthwatch, run the following command: **Authorizer.py -l**  
  Refer to **Command Line Interface** |
To enable authorization for a specific TACACS+ server, refer to 2. Add the TACACS+ Server to Stealthwatch for details.

When a user logs in, they can only access the SMC locally. If a user exists with the same user name in Stealthwatch (local) and the TACACS+ server (remote), the local login overrides the remote login. Refer to User Roles Overview for details.

Command Line Interface Authorization Help

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable authorization service</td>
<td>Authorizer.py -e SERVICE</td>
</tr>
<tr>
<td></td>
<td>Refer to 2. Add the TACACS+ Server to Stealthwatch for details.</td>
</tr>
<tr>
<td>To enable a specific TACACS+ server:</td>
<td>Authorizer.py -e &lt;TACACS+ server name&gt;</td>
</tr>
<tr>
<td>Disable authorization service</td>
<td>Authorizer.py -d SERVICE</td>
</tr>
<tr>
<td></td>
<td>Refer to Disabling Authorization for details.</td>
</tr>
<tr>
<td>Help</td>
<td>Authorizer.py -h</td>
</tr>
<tr>
<td>List services</td>
<td>Authorizer.py -l</td>
</tr>
<tr>
<td>Show absolute path to authentication service file</td>
<td>Authorizer.py -f FILE</td>
</tr>
</tbody>
</table>
Contacting Support

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

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
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)