Configure and Troubleshoot External TACACS Servers on ISE

Contents

Introduction

This document describes the feature to utilize the External TACACS+ Server in a deployment using Identity Service Engine(ISE) as a proxy.

Prerequisites

Requirements

- Basic understanding of Device Administration on ISE.
- This document is based on Identity Service Engine version 2.0, applicable on any version of Identity Service Engine verison higher than 2.0.

Components Used

> **Note**: Any reference to ACS in this document can be interpretted to be a reference to any External TACACS+ Server. However, configuration on the ACS and the configuration on any other TACACS Server may vary.

The information in this document is based on these software and hardware versions:

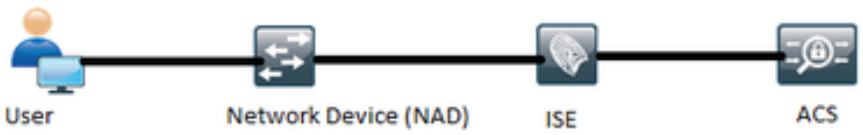
- Identity Service Engine 2.0
- Access Control System (ACS) 5.7

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, make sure that you understand the potential impact of any configuration change.

Configure

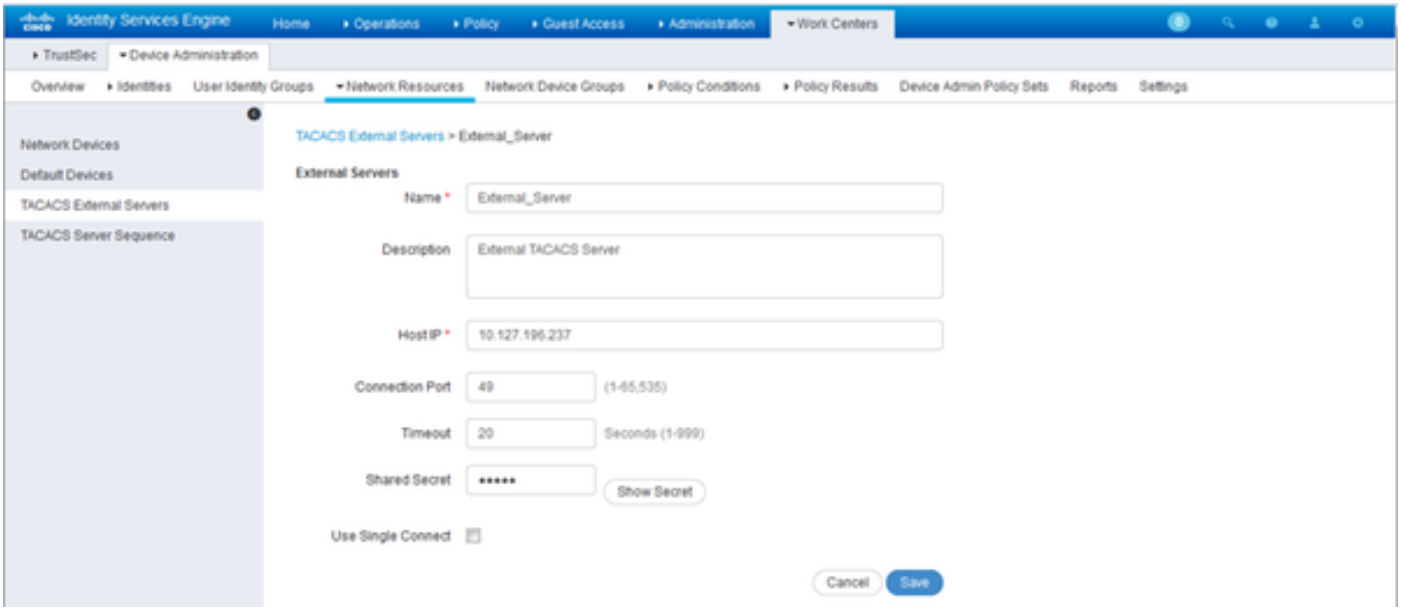
This section helps to configure ISE to proxy TACACS+ requests to ACS.

Network Diagram



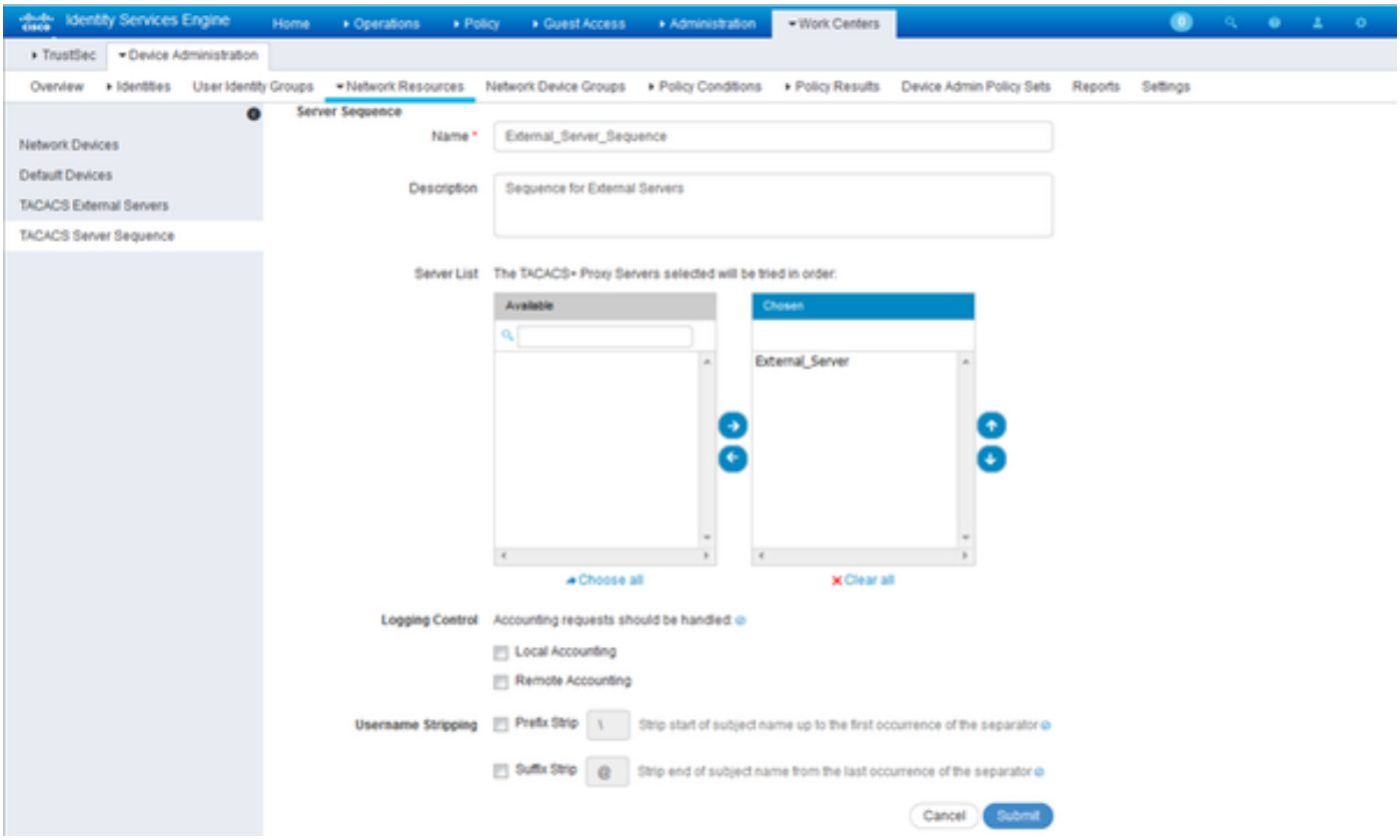
Configure ISE

1. Multiple External TACACS Servers can be configured on ISE and can be used to authenticate the users. In order to configure External TACACS+ Server on ISE, navigate to **Work Centers > Device Administration > Network Resources > TACACS External Servers.** Click **Add** and fill in the details of the External Server Details.



The shared secret provided in this section must be the same secret used in the ACS.

2. In order to utilize the External TACACS Server configured, it must be added in a TACACS Server sequence to be used in the policy sets. I order to configure TACACS Server Sequence, navigate to **Work Centers > Device Administration > Network Resources > TACACS Server Sequence.** Click **Add,** fill in the details and choose the servers that are needed to be used in that sequence.

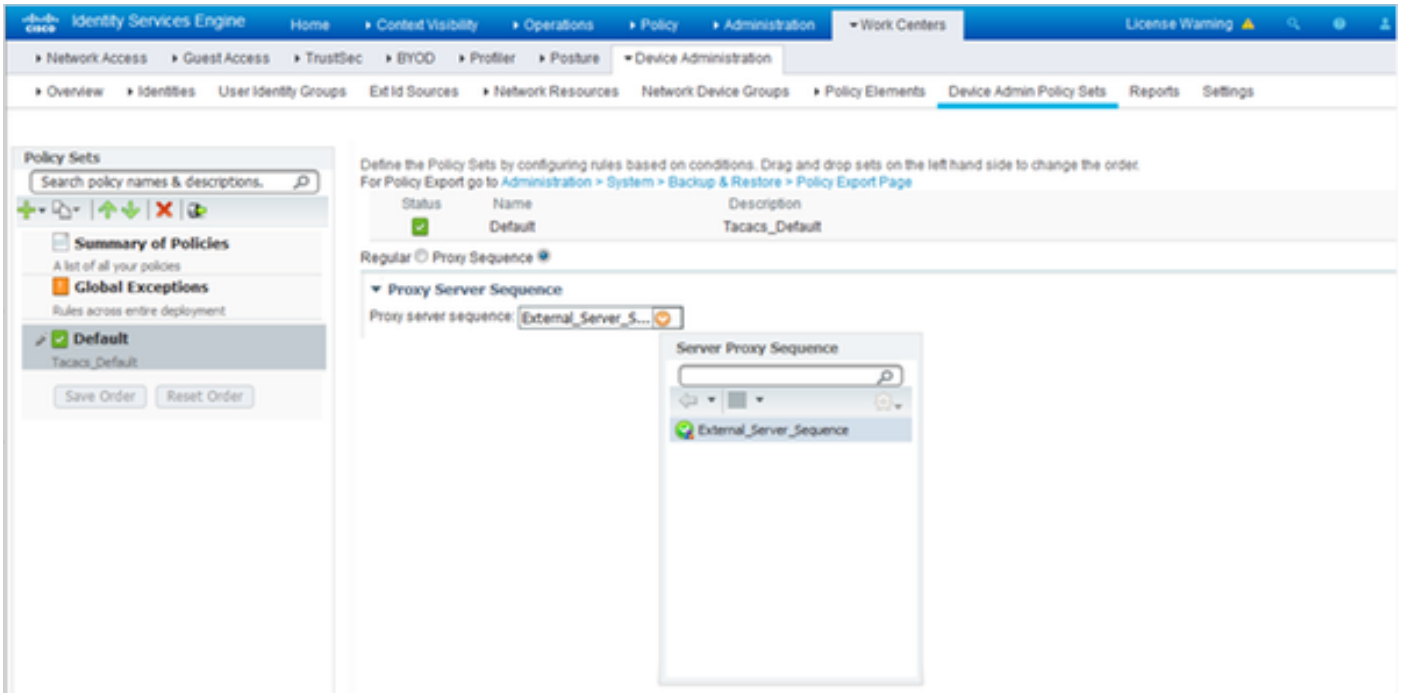


In addition to the server sequence, two other options have been provided. Logging Control and Username Stripping.

Logging Control gives an option to either log the accounting requests locally on ISE or log the accounting requests to the external server which handles the authentication as well.

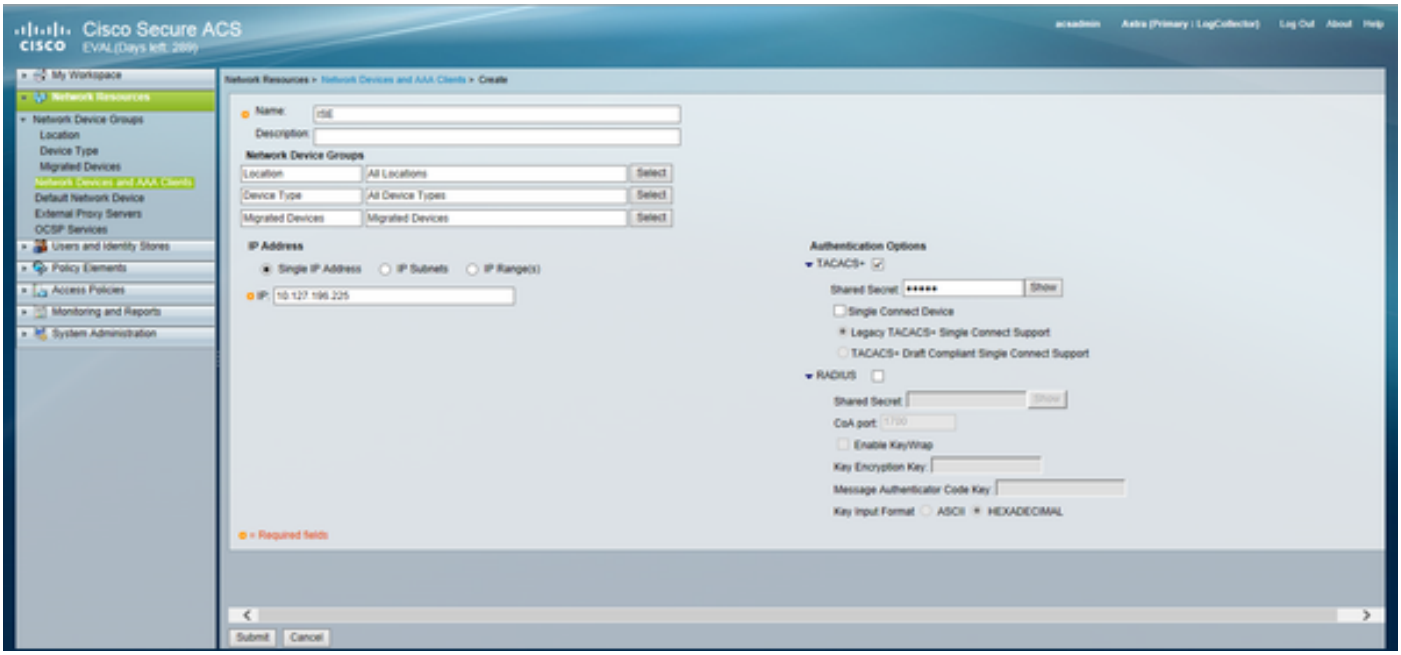
Username Stripping is used to strip either the Prefix or the Suffix by sepcifying a delimiter before forwarding the request to an External TACACS Server.

3. To utilize the External TACACS Server Sequence configured, the policy sets must be configured to use the sequence created. In order to configure the policy sets to use the External Server Sequence, navigate to **Work Centers > Device Administration > Device Admin Policy Sets > [select the policy set].** Toggle radio button which says **Proxy Sequence.** Choose the External Server Sequence created.

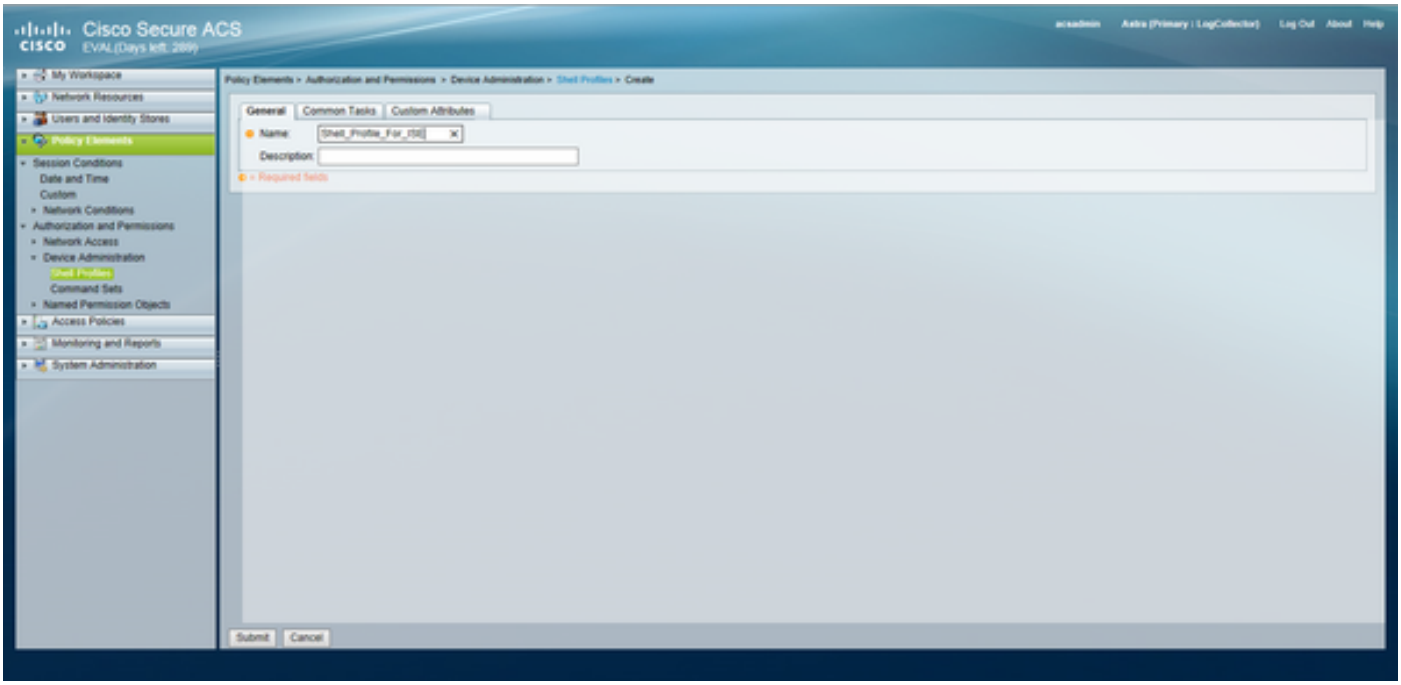


Configure ACS

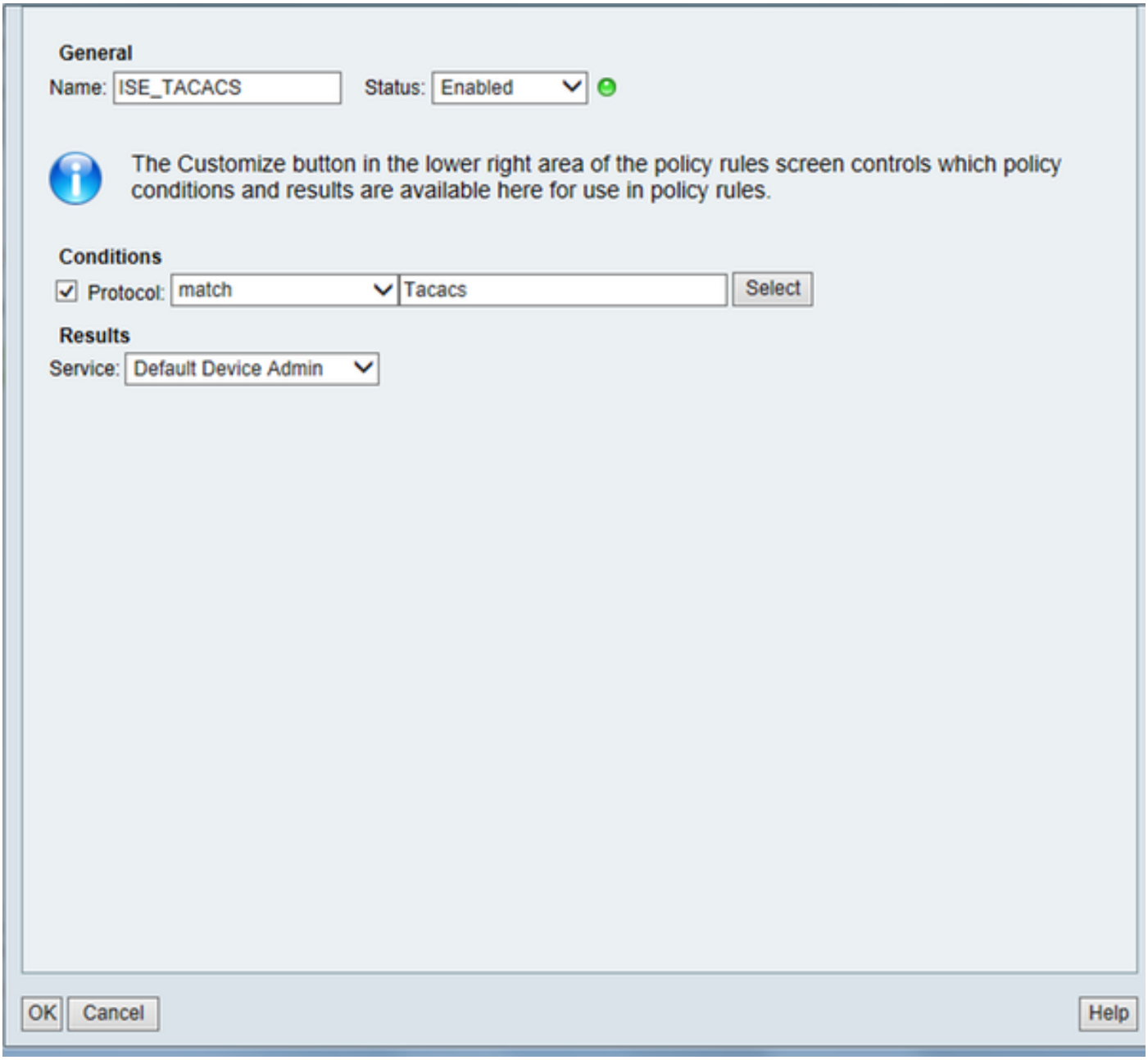
For the ACS, ISE is just another Network Device which will be sending a TACACS Request. In order to configure ISE as a network device in ACS, navigate to **Network Resources > Network Devices and AAA Clients.** Click **Create** and fill in the details of the ISE Server using the same shared secret as configured on the ISE.



Configure Device Administration Parameters on ACS which are, the shell profiles and the command sets. In order to configure Shell Profiles, navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles.** Click **Create** and configure the name, Common Tasks and Custom Attributes as per the requirement.



In order to conofigure Command Sets, navigate to **Policy Elements > Authorization and Permissions > Device Administration > Command Sets.** Click **Create** and fill in the details as per the requirement.



Configure the Access Service Selected in the Service Selection rule as per the requirement.In order to configure Access Service Rules, navigate to **Access Policies > Access Services >Default Device Admin > Identity** where the identity store that needs to be used can be selected for authentication. The authorization rules can be configured by navigating to **Access Policies > Access Services >Default Device Admin > Authorization.**

> **Note**: Configuration of the authorization policies and shell profles for specific devices may vary and that is out of the scope of this document.

Verify

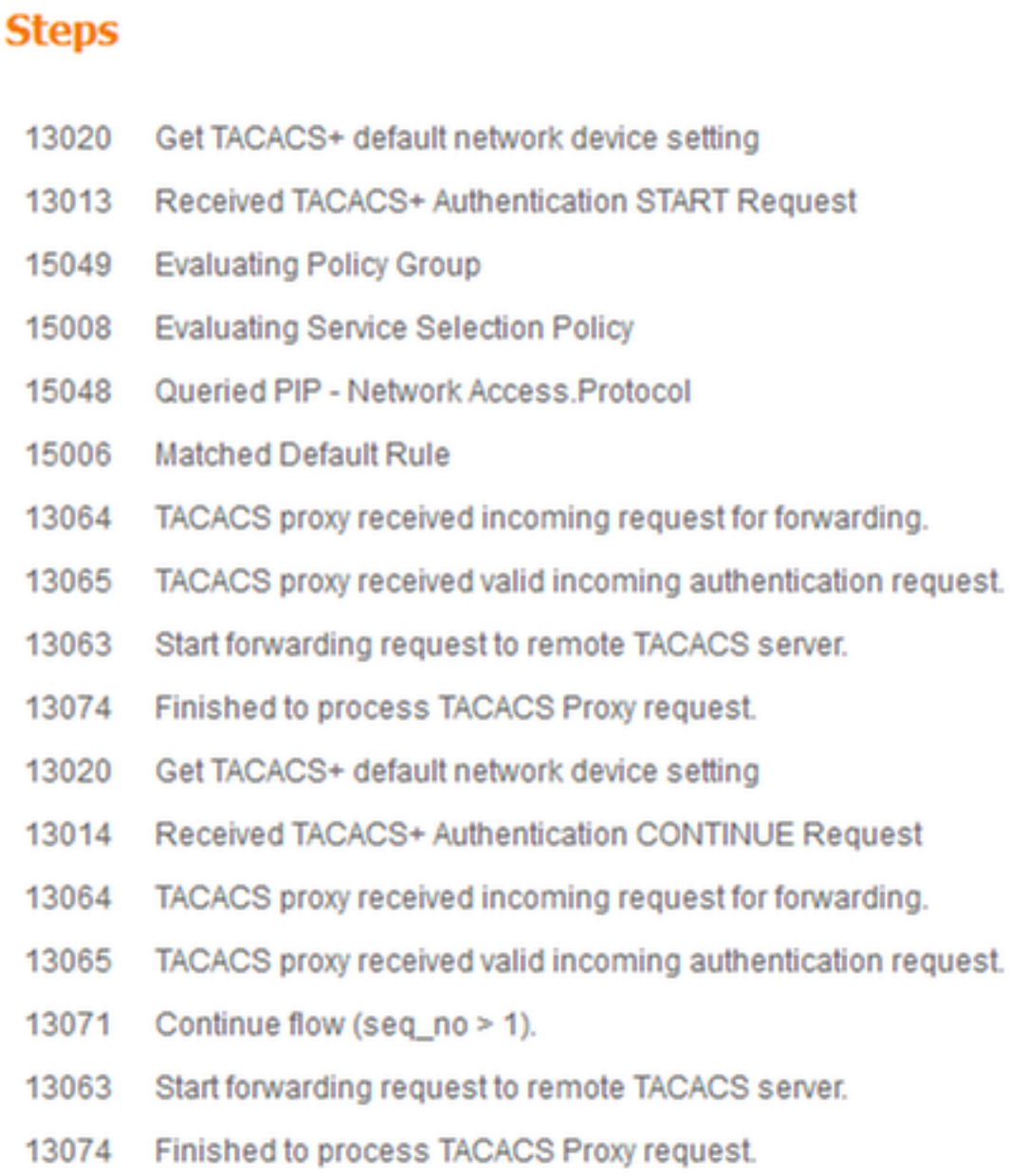
Use this section to confirm that the configuration works properly.

Verification can be done on both the ISE and the ACS. Any mistake in the configuration of the ISE or the ACS will result in an authentication failure. ACS is the primary server that will handle the authentication and the authorization requests, ISE bears the responsibility to and from the ACS server and act as a proxy for the requests. Since the packet traverses through both the servers,

verification of the authentication or the authorization request can be done on both the servers.

Network devices are configured with ISE as TACACS server and not the ACS. Hence the request reaches ISE first and based upon the rules configured, ISE decides if the request needs to be forwarded to an external server. This can be verified in the TACACS Live logs on the ISE.

In order to view the live logs on the ISE, navigate to **Operations > TACACS > Live Logs.** Live reports can be seen on this page and the details of a particular request can be checked by clicking the magnifying glass icon pertaining to that specific request that is of interest.

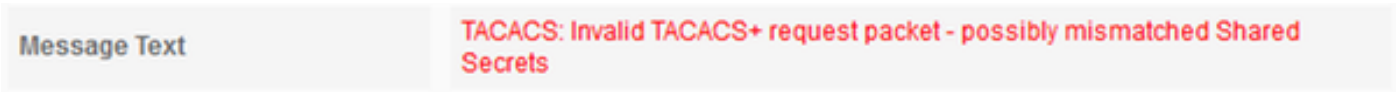


In order to view the authentication reports on the ACS, navigate to **Monitoring and Reports > Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > AAA Protocol > TACACS Authentication.** Like ISE, the details of a particular request can be checked by clicking the magnifying glass icon pertaining to that specific request that is of interest

Troubleshoot

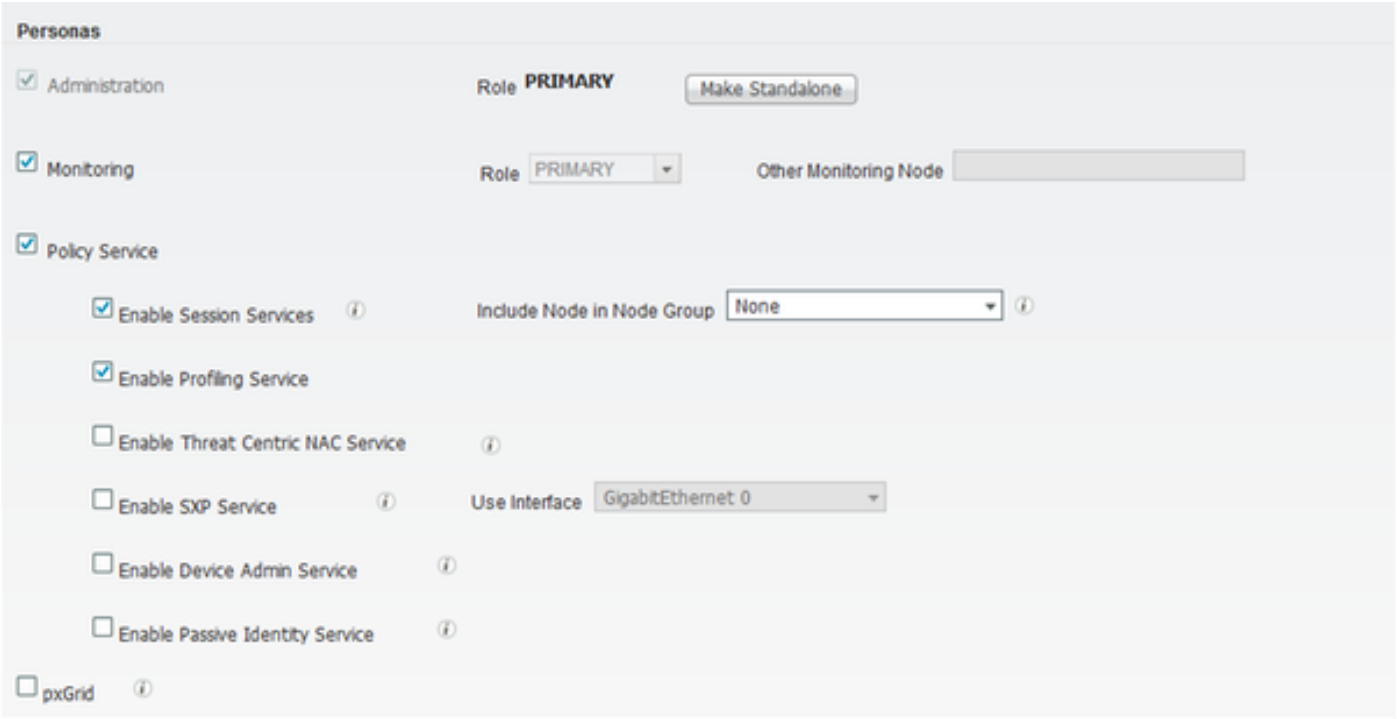
This section provides information you can use to troubleshoot your configuration

1. If the details of the report on ISE show the error message shown in the figure, then it indicates an invalid shared secret configured on either the ISE or the Netowrk Device (NAD).

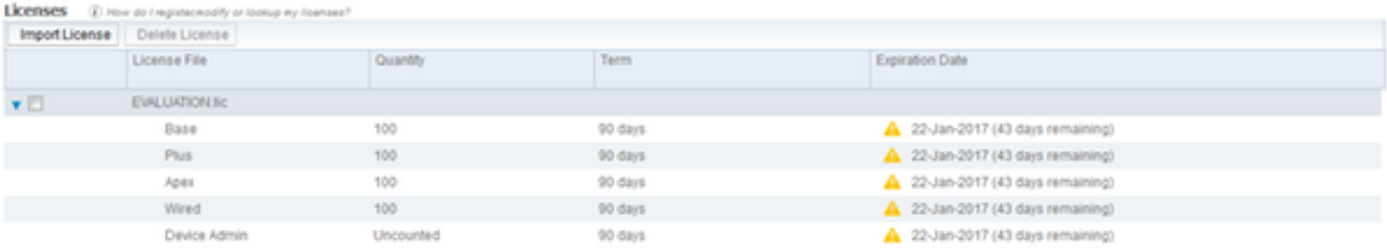


2. If there is no authentication report for a request on the ISE but the access is being denied to the end user to a network device, this usually indicates several things.

- The request itself did no reach the ISE server.
- If the Device Administration persona is disabled on ISE, then any TACACS+ request to ISE willbe dropped silently. No logs indicating the same will be shown in the reports or the Live Logs. To verify this, navigate to **Administration > System > Deployment > [select the node].** Click **Edit** and notice the "**Enable Device Admin Service**" check box under the **General Settings** tab as shown in the figure. That checkbox needs to be checked for the Device Administration to work on ISE.



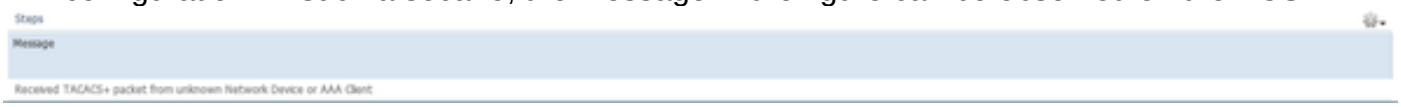
- If a Device Administration license is not present of expired, then all the TACACS+ requests are dropped silently. No logs are shown in the GUI for the same. Navigate to **Administration > System > Licensing** to check the device administration license**.**



- If the network device is not configured or if a wrong network device IP is configured on the ISE, then ISE will silently drop the packet. No response is sent back to the client and no logs are shown in the GUI. This is a change of behaviour in ISE for TACACS+ when compared to that of ACS which informs that the request came in from an unkown Network Device or AAA Client.

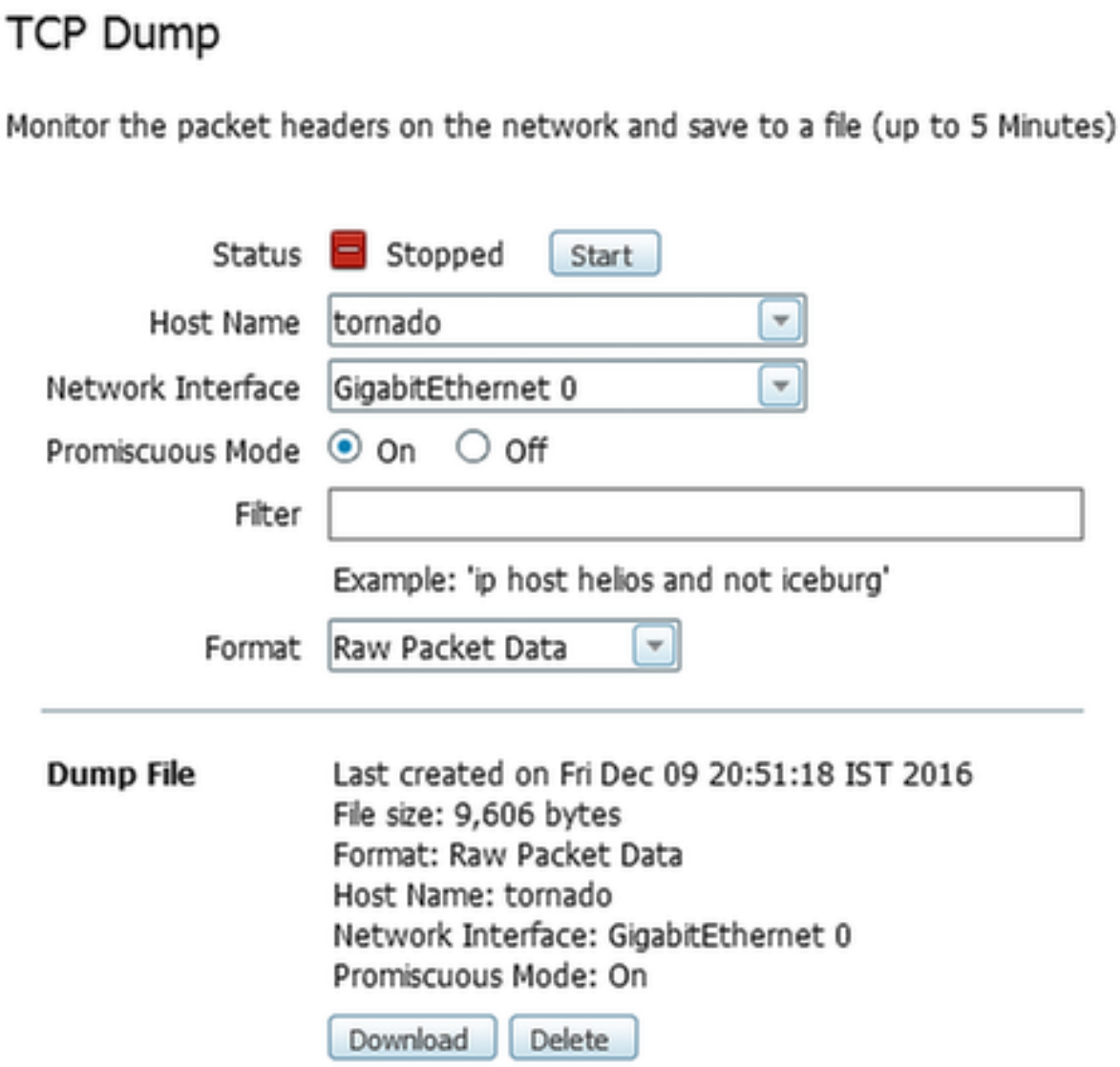
- The request reached the ACS but the response did not come back to the ISE. This scenario can be checked from the reports on the ACS as shown in the figure. Usually this is becuase of an invalid shared secret either on the ACS configured for ISE or on the ISE configured for the ACS.

- The response will not be sent even if the ISE is not configured or the IP address of the Management interface of ISE is not configured on the ACS in the Network Device configuration. In such a secario, the message in the figure can be observed on the ACS.



- If a successful authentication report is seen on the ACS but no reports are seen on the ISE

and the user is being rejected, then it could very well be an issue in the network. This can be verified by a packet capture on ISE with necessary filters. To collect a packet capture on ISE, navigate to **Operations > Troubleshoot > Diagnostic Tools > General tools > TCP Dump.**



3. If the reports can be seen on ISE but not on the ACS, it could either mean that the request has not reached the ACS because of a misconfiguration of the Policy Sets on ISE which can be troubleshooted based on the detailed report on ISE or because of a network issue which can be identified by a packet capture on the ACS.

4. If the reports are seen on both ISE and the ACS but user is still being denied access, then it is more often an issue in the Access Policies configuration on ACS which can be troubleshooted based upon the detailed report on the ACS. Also, the return traffic from the ISE to the Netowork Device must be allowed.