This document describes how to configure TACACS+ Authentication and Authorization for the Firepower eXtensible Operating System (FXOS) chassis via Identity Services Engine (ISE).

The FXOS chassis includes the following User Roles:

- **Administrator** - Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.
- **Read-Only** - Read-only access to system configuration with no privileges to modify the system state.
- **Operations** - Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.
- **AAA** - Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Via CLI this can be seen as follows:

```
fpr4120-TAC-A /security* # show role
```

Role:
<table>
<thead>
<tr>
<th>Role Name</th>
<th>Priv</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------</td>
<td>----</td>
</tr>
<tr>
<td>aaa</td>
<td>aaa</td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>operations</td>
<td>operations</td>
</tr>
<tr>
<td>read-only</td>
<td>read-only</td>
</tr>
</tbody>
</table>

Contributed by Tony Remirez, Jose Soto, Cisco TAC Engineers.

**Prerequisites**

**Requirements**

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower eXtensible Operating System (FXOS)
- Knowledge of ISE configuration
- TACACS+ Device Administration license is required within ISE

**Components Used**

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

- Cisco Firepower 4120 Security Appliance version 2.2
- Virtual Cisco Identity Services Engine 2.2.0.470

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 command.

**Configure**

The goal of the configuration is to:

- Authenticate users logging into the FXOS’s Web-based GUI and SSH by means of ISE
- Authorize users logging into the FXOS’s Web-based GUI and SSH according to their respective User Role by means of ISE.
- Verify the proper operation of authentication and authorization on the FXOS by means of ISE

**Network Diagram**
Configurations

Configuring the FXOS Chassis

Creating a TACACS+ Provider

Step 1. Navigate to Platform Settings > AAA.

Step 2. Click the TACACS tab.

Step 3. For each TACACS+ provider that you want to add (Up to 16 providers).

3.1. In TACACS Providers area, click Add.

3.2. Once the Add TACACS Provider dialog box opens, enter the required values.

3.3. Click OK to close the Add TACACS Provider dialog box.
Step 4. Click **Save**.

Step 5. Navigate to **System > User Management > Settings**.

Step 6. Under Default Authentication choose **TACACS**.

**Creating a TACACS+ Provider using CLI**

Step 1. In order to enable TACACS authentication run the following commands.

```
fpr4120-TAC-A# scope security
```
fpr4120-TAC-A /security # scope default-auth
fpr4120-TAC-A /security/default-auth # set realm tacacs

Step 2. Use the **show detail** command to verify the configuration.

fpr4120-TAC-A /security/default-auth # show detail

Default authentication:

  Admin Realm: **Tacacs**
  Operational Realm: **Tacacs**
  Web session refresh period(in secs): 600
  Session timeout(in secs) for web, ssh, telnet sessions: 600
  Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
  Serial Console Session timeout(in secs): 600
  Serial Console Absolute Session timeout(in secs): 3600
  Admin Authentication server group:
  Operational Authentication server group:
  Use of 2nd factor: No

Step 3. In order to configure TACACS server parameters run the following commands.

fpr4120-TAC-A# scope security
fpr4120-TAC-A /security # scope tacacs
fpr4120-TAC-A /security/tacacs # enter server 10.88.244.50
fpr4120-TAC-A /security/tacacs/server # set descr "ACS Server"

fpr4120-TAC-A/ security/tacacs/server# # set key

Enter the key: ******
Confirm the key: ******

Step 4. Use the **show detail** command to verify the configuration.

fpr4120-TAC-A/ security/tacacs/server# # show detail

TACACS+ server:

  Hostname, FQDN or IP address: 10.88.244.50
Configuring the ISE server

Adding the FXOS as a network resource

Step 1. Navigate to Administration > Network Resources > Network Devices.

Step 2. Click ADD.

Step 3. Enter the required values (Name, IP Address, Device Type and Enable TACACS+ and add the KEY), click Submit.
Creating the Identity groups and Users

Step 1. Navigate to **Administration > Identity Management > Groups > User Identity Groups**.

Step 2. Click **ADD**.
Step 3. Enter the value for Name and click **Submit**.

Step 4. Repeat step 3 for all the required User Roles.

Step 5. Navigate to **Administration > Identity Management > Identity > Users**.

Step 6. Click **ADD**.

Step 7. Enter the required values (Name, User Group, Password).
Step 8. Repeat step 6 for all required users.

Creating the Shell Profile for each User Role

Step 1. Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles and click +ADD.
Step 2. Enter the required values for the TACACS Profile

2.1. Enter the Name.

2.2. In **RAW View** TAB configure the following CISCO-AV-PAIR.

```
cisco-av-pair=shell:roles="admin"
```
2.3. Click **Submit**.
Step 3. Repeat step 2 for the remaining User Roles using the following Cisco-AV-Pairs.

\texttt{cisco-av-pair=shell:roles="aaa"}  
\texttt{cisco-av-pair=shell:roles="operations"}  
\texttt{cisco-av-pair=shell:roles="read-only"}
Creating the TACACS Authorization Policy

Step 1. Navigate to Work Centers > Device Administration > Device Admin Policy Sets.

Step 2. Ensure that the Authentication Policy points to the Internal Users database or the required Identity Store.
Step 3. Click the arrow at the end of the default Authorization policy and click insert rule above.

Step 4. Enter the values for the rule with the required parameters:

4.1. Rule Name: FXOS Admin Rule.

4.2. Conditions.

   If : User Identity Group is FXOS ADMIN

   And Device: Device Type equals All Device Types #FXOS
Step 5. Click **Done**.
Step 6. Repeat step 3 and 4 for the remaining user roles and when finished click SAVE.

Verify

You may now test each user and verify the assigned User Role.

FXOS Chasis verification

1. Telnet or SSH to the FXOS Chassis and login using any of the created users on the ISE.

Username: fxosadmin

Password:

fpr4120-TAC-A# scope security

fpr4120-TAC-A /security # show remote-user detail

Remote User fxosaaa:
Description:
User Roles:
   Name: aaa
   Name: read-only
Remote User fxosadmin:
Description:
User Roles:
   Name: admin
   Name: read-only
Remote User fxosoper:
Description:
User Roles:
   Name: operations
   Name: read-only
Remote User fxosro:
Description:
User Roles:
   Name: read-only
Depending on the username entered the FXOS chassis cli will only display the commands authorized for the User Role assigned.
Admin User Role.
fpr4120-TAC-A /security #
   acknowledge    Acknowledge
   clear-user-sessions  Clear User Sessions
   create    Create managed objects
   delete    Delete managed objects
   disable   Disables services
enable Enables services
enter Enters a managed object
scope Changes the current mode
set Set property values
show Show system information
terminate Active cimc sessions

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa aaa-requests

fpr4120-TAC-A (fxos)#

Read-Only User Role.

fpr4120-TAC-A /security # ?

scope Changes the current mode
set Set property values
show Show system information

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa aaa-requests

% Permission denied for the role

2. Browse to the FXOS Chassis IP address and login using any of the created users on the ISE.

Admin User Role.

Read-only User Role.
Note: Notice that the ADD button is greyed out.

ISE 2.0 Verification

1. Navigate to Operations > TACACS Livelog. You should be able to see successful and failed attempts.

Troubleshoot

In order to debug AAA authentication and authorization run the following commands in the FXOS cli.

fpr4120-TAC-A# connect fxos

fpr4120-TAC-A (fxos)# debug aaa aaa-requests

fpr4120-TAC-A (fxos)# debug aaa event

fpr4120-TAC-A (fxos)# debug aaa errors

fpr4120-TAC-A (fxos)# term mon

After a successful authentication attempt, you will see the following output.

2018 Jan 17 15:46:40.305247 aaa: aaa_req_process for authentication. session no 0

2018 Jan 17 15:46:40.305262 aaa: aaa_req_process: General AAA request from appln: login appln_subtype: default

2018 Jan 17 15:46:40.305271 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.305285 aaa: total methods configured is 1, current index to be tried is 0

2018 Jan 17 15:46:40.305294 aaa: handle_req_using_method
2018 Jan 17 15:46:40.305301 aaa: AAA_METHOD_SERVER_GROUP
2018 Jan 17 15:46:40.305308 aaa: aaa_sg_method_handler group = tacacs
2018 Jan 17 15:46:40.305315 aaa: Using sg_protocol which is passed to this function
2018 Jan 17 15:46:40.305324 aaa: Sending request to TACACS service
2018 Jan 17 15:46:40.305384 aaa: Configured method group Succeeded
2018 Jan 17 15:46:40.554631 aaa: aaa_process_fd_set
2018 Jan 17 15:46:40.555229 aaa: aaa_process_fd_set: mtscallback on aaa_q
2018 Jan 17 15:46:40.556387 aaa: prot_daemon_reponse_handler
2018 Jan 17 15:46:40.557042 aaa: session: 0x8dfd68c removed from the session table 0
2018 Jan 17 15:46:40.557059 aaa: is_aaa_resp_status_success status = 1
2018 Jan 17 15:46:40.557066 aaa: is_aaa_resp_status_success is TRUE
2018 Jan 17 15:46:40.557083 aaa: AAA_REQ_FLAG_NORMAL
2018 Jan 17 15:46:40.557106 aaa: mts_send_response Successful
2018 Jan 17 15:46:40.557364 aaa: aaa_req_process for authorization. session no 0
2018 Jan 17 15:46:40.557378 aaa: aaa_req_process called with context from appln: login appln_subtype: default authen_type:2, authen_method: 0
2018 Jan 17 15:46:40.557386 aaa: aaa_send_req_using_context
2018 Jan 17 15:46:40.557394 aaa: aaa_sg_method_handler group = (null)
2018 Jan 17 15:46:40.557401 aaa: Using sg_protocol which is passed to this function
2018 Jan 17 15:46:40.557408 aaa: context based or directed AAA req(exception: not a relay request). Will not take copy of aaa request
2018 Jan 17 15:46:40.557415 aaa: Sending request to TACACS service
2018 Jan 17 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAL
2018 Jan 17 15:46:40.801761 aaa: mts_send_response Successful
2018 Jan 17 15:46:40.848932 aaa: OLD OPCODE: accounting_interim_update

2018 Jan 17 15:46:40.848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=added user:fxosadmin to the role:admin

2018 Jan 17 15:46:40.848963 aaa: aaa_req_process for accounting. session no 0

2018 Jan 17 15:46:40.848972 aaa: MTS request reference is NULL. LOCAL request

2018 Jan 17 15:46:40.848982 aaa: Setting AAA_REQ_RESPONSE_NOT_NEEDED

2018 Jan 17 15:46:40.848992 aaa: aaa_req_process: General AAA request from appln: default appln_subtype: default

2018 Jan 17 15:46:40.849002 aaa: try_next_aaa_method

2018 Jan 17 15:46:40.849022 aaa: no methods configured for default default

2018 Jan 17 15:46:40.849032 aaa: no configuration available for this request

2018 Jan 17 15:46:40.849043 aaa: try_fallback_method

2018 Jan 17 15:46:40.849053 aaa: handle_req_using_method

2018 Jan 17 15:46:40.849063 aaa: local_method_handler

2018 Jan 17 15:46:40.849073 aaa: aaa_local_accounting_msg

2018 Jan 17 15:46:40.849085 aaa: update:::added user:fxosadmin to the role:admin

After a failed authentication attempt, you will see the following output.

2018 Jan 17 15:46:17.836271 aaa: aaa_req_process for authentication. session no 0


2018 Jan 17 15:46:17.837063 aaa: try_next_aaa_method

2018 Jan 17 15:46:17.837416 aaa: total methods configured is 1, current index to be tried is 0


2018 Jan 17 15:46:17.838103 aaa: AAA_METHOD_SERVER_GROUP

2018 Jan 17 15:46:17.838477 aaa: aaa_sg_method_handler group = tacacs

2018 Jan 17 15:46:17.838826 aaa: Using sg_protocol which is passed to this function

2018 Jan 17 15:46:17.839167 aaa: Sending request to TACACS service

2018 Jan 17 15:46:17.840225 aaa: Configured method group Succeeded
2018 Jan 17 15:46:18.043710 aaa: is_aaa_resp_status_success status = 2
2018 Jan 17 15:46:18.044048 aaa: is_aaa_resp_status_success is TRUE
2018 Jan 17 15:46:18.044733 aaa: AAA_REQ_FLAG_NORMAL
2018 Jan 17 15:46:18.045096 aaa: mts_send_response Successful
2018 Jan 17 15:46:18.045677 aaa: aaa_cleanup_session
2018 Jan 17 15:46:18.045689 aaa: mts_drop of request msg
2018 Jan 17 15:46:18.045699 aaa: aaa_req should be freed.
2018 Jan 17 15:46:18.045715 aaa: aaa_process_fd_set
2018 Jan 17 15:46:18.045722 aaa: aaa_process_fd_set: mtscallback on aaa_q
2018 Jan 17 15:46:18.045732 aaa: aaa_enable_info_config: GET_REQ for aaa login error message
2018 Jan 17 15:46:18.045738 aaa: got back the return value of configuration operation:unknown security item

Related Information

Ethanalyzer command on FX-OS cli will prompt for password for a password when TACACS/RADIUS authentication is enabled. This behavior is caused by a bug.

Bug id: CSCvg87518