



TACACS+ Configuration Examples

Avi Technical Reference (v17.2)

Copyright © 2018

TACACS+ Configuration Examples

[view online](#)

ISE TACACS+ Server

Cisco ISE is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations.

Given below are steps involved in setting up an ISE TACACS+ server as a remote authentication and authorization system for Avi Vantage.

- The ISE server is generally configured with external Identity Sources (in this case OpenLDAP).

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for an Authentication Policy. The page is titled "Authentication Policy" and includes the following configuration options:

- Policy Type:** Simple Rule-Based
- Network Access Service:** Allowed Protocol : Default Device A... (dropdown menu)
- Identity Source:** OpenLDAP (dropdown menu)
- Options:**
 - If authentication failed: Reject (dropdown menu)
 - If user not found: Reject (dropdown menu)
 - If process failed: Drop (dropdown menu)

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation at the top reads: Home > Operations > Policy > Guest Access > Administration > Work Centers > Identity Management > External Identity Sources > Identity Source Sequences > Settings. The left sidebar, titled "External Identity Sources", contains a tree view with categories like Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token, RSA SecurID, and SAML Id Providers. The "LDAP" category is expanded, and "OpenLDAP" is selected. The main content area is titled "LDAP Identity Sources List > OpenLDAP" and "LDAP Identity Source". It features a tabbed interface with "General" selected. The configuration fields include: Name (OpenLDAP), Description (empty), Schema (Custom), Subject Objectclass (inetOrgPerson), Group Objectclass (posixGroup), Subject Name Attribute (uid), Group Map Attribute (memberUid), and Certificate Attribute (empty). At the bottom, there are radio buttons for "Subject Objects Contain Reference To Groups" (unselected) and "Group Objects Contain Reference To Subjects" (selected), and a dropdown for "Subjects In Groups Are Stored In Member Attribute As" set to "Username".

LDAP Identity Sources List > [OpenLDAP](#)

LDAP Identity Source

General **Connection** Directory Organization Groups Attributes

Primary Server	Secondary Server
<input type="checkbox"/> Enable Secondary Server	
* Hostname/IP <input type="text" value="10.10.23.120"/> ⓘ	Hostname/IP <input type="text"/> ⓘ
* Port <input type="text" value="389"/>	Port <input type="text" value="389"/>
Access <input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access <input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN * <input type="text" value="cn=admin,dc=example,dc=com"/>	Admin DN <input type="text"/>
Password * <input type="password" value="*****"/>	Password <input type="password"/>
Secure Authentication <input type="checkbox"/> Enable Secure Authentication <input type="checkbox"/> Enable Server Identity Check	Secure Authentication <input type="checkbox"/> Enable Secure Authentication <input type="checkbox"/> Enable Server Identity Check
LDAP Server Root CA <input type="text" value="Thawte Primary Root CA"/> ⓘ	LDAP Server Root CA <input type="text" value="Thawte Primary Root CA"/> ⓘ
Issuer CA of ISE Certificate <input type="text" value="Select if required (optional)"/> ⓘ	Issuer CA of ISE Certificate <input type="text" value="Select if required (optional)"/> ⓘ

LDAP Identity Sources List > [OpenLDAP](#)

LDAP Identity Source

General Connection **Directory Organization** Groups Attributes

* Subject Search Base ⓘ

* Group Search Base ⓘ

Search for MAC Address in Format

Strip start of subject name up to the last occurrence of the separator

Strip end of subject name from the first occurrence of the separator

- ISE LDAP settings used to fetch LDAP groups in order to use them for Authorization conditions

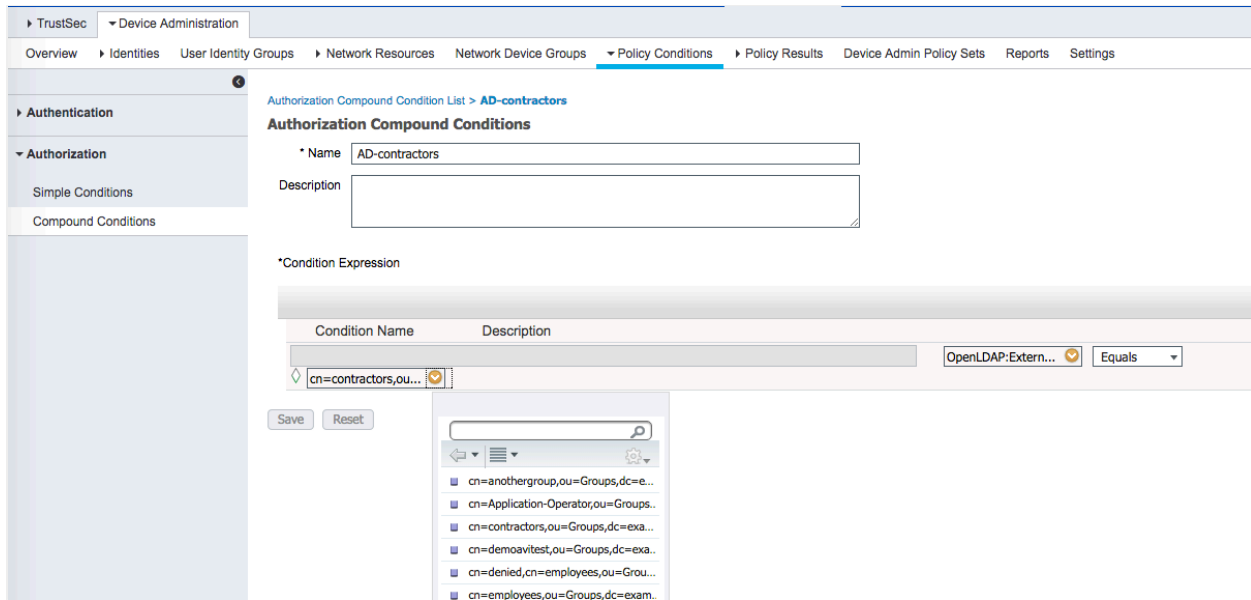
The screenshot shows the 'LDAP Identity Sources List > OpenLDAP' configuration page. The 'LDAP Identity Source' is selected, and the 'Groups' tab is active. The interface includes tabs for 'General', 'Connection', 'Directory Organization', 'Groups', and 'Attributes'. Below the tabs, there are action buttons: 'Edit', '+ Add', and 'X Delete Group'. A table lists the following LDAP groups:

<input type="checkbox"/>	Name
<input type="checkbox"/>	cn=Application-Operator,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=LDAP-Group1,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=anothergroup,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=contractors,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=demoavitest,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=denied,cn=employees,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=employees,ou=Groups,dc=example,dc=com
<input type="checkbox"/>	cn=partners,ou=Groups,dc=example,dc=com

- ISE Authorization conditions added for Users in the AD groups

The screenshot shows the 'Identity Services Engine' interface. The navigation path is: Administration > Policy Conditions > Authorization Compound Conditions. The page title is 'Authorization Compound Condition List >'. Below the title, there are instructions: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Action buttons include 'Edit', '+ Add', 'Duplicate', and 'X Delete'. A table lists the following authorization conditions:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	AD-contractors	
<input type="checkbox"/>	AD-employees	
<input type="checkbox"/>	BYOD_is_Registered	



- ISE server should recognize all Avi Vantage Controller cluster nodes as valid Network Devices.

Identity Services Engine | Home | Operations | Policy | Guest Access | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Identity Mapping

Network Devices | Network Device Groups | **Network Device Profiles** | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External

Network Device Profile List > **AviController** Save Reset

Network Device Profile

* Name:

Description:

Icon: Change icon... Set To Default ?

Vendor:

Supported Protocols

RADIUS

TACACS+

TrustSec

RADIUS Dictionaries:

Templates

[Expand All / Collapse All](#)

- ▶ **Authentication/Authorization**
- ▶ **Permissions**
- ▶ **Change of Authorization (CoA)**
- ▶ **Redirect**

The screenshot displays the configuration interface for a network device in Cisco ISE. The breadcrumb navigation shows: Home > Operations > Policy > Guest Access > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Identity Mapping > Network Devices. The left sidebar shows a tree view with 'Network devices' selected. The main content area is titled 'Network Devices List > AviControllers' and 'Network Devices'. The configuration fields are as follows:

- Name:
- Description:
- * IP Address: /
- * Device Profile:
- Model Name:
- Software Version:
- * Network Device Group
 - Location:
 - Device Type:
- RADIUS Authentication Settings
- TACACS+ Authentication Settings
 - Shared Secret:
 - Enable Single Connect Mode
 - Legacy Cisco Device
 - TACACS+ Draft Compliance Single Connect Support

- ISE requires shell profiles and TACACS+ profiles configured.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Device Administration > Policy Results > TACACS Profiles. The main content area shows a table of TACACS Profiles with the following data:

Name	Description
Default Shell Profile	Default Shell Profile
ShellProfileRO	
ShellProfileRW	

The screenshot shows the configuration details for the TACACS Profile 'ShellProfileRW'. The Name field is set to 'ShellProfileRW'. The Description field is empty. Below the form, there are two tabs: 'Task Attribute View' and 'Raw View'. The 'Raw View' is selected, showing the following profile attributes:

```
priv-lvl=15
aviRole=read-write
```

- ISE device policy sets default condition updated to assign different shell profiles based on group membership.

Overview | Identities | User Identity Groups | Network Resources | Network Device Groups | Policy Conditions | Policy Results | **Device Admin Policy Sets** | Reports | Settings

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Default
Tacacs_Default

Save Order | Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

Proxy Server Sequence
Proxy server sequence:

Authentication Policy

Default Rule (if no match) : Allow Protocols : Default Device Admin and use : OpenLDAP

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	PermitShowCommands	if AD-contractors	then PermitShowCommands AND ShellProfileRO	
<input checked="" type="checkbox"/>	PermitAllCommands	if AD-employees	then PermitAllCommands AND ShellProfileRW	
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands AND Default Shell Profile	

- The Avi Vantage TACACS+ auth profile should be configured with the same shared secret that was assigned to the device in ISE. The "service" attribute is generally required for authorization. In the case of an ACS server, service=shell is required for user authorization; while in the case of an ISE server, service=shell is known to cause authorization failure.

Edit Auth Profile: ISE Tacacs server

Name * Type TACACS+

TACACS+ Servers Port

+ Add Item

Password TACACS+ Service

TACACS+ Authorization Attributes

Name	Value	Mandatory
service	avishell	<input checked="" type="checkbox"/>

+ Add Attribute

- **Avi Vantage TACACS+ authorization role and tenant mapping configured to assign different roles based on TACACS+ attribute value**

The screenshot displays the Avi Vantage Administration interface. The top navigation bar includes 'Administration', 'Accounts', 'Settings', 'Controller', 'System Upgrade', and 'GSLB'. The 'Settings' tab is active, and the breadcrumb trail shows 'Authentication/Authorization'. Below the breadcrumb, there are links for 'Access Settings', 'DNS / NTP', 'Licensing', 'Email/SMTP', 'Tenant Settings', 'SSH Key Settings', and 'Upload HSM Packages'. The main content area shows 'Authentication/Authorization: TACACS+' and 'Profile: ISE Tacacs server'. Below this, the 'Tenant and Role Mapping' section is visible, featuring a 'New Mapping' button and a search bar. A table displays two mappings:

Authorization	Assignment
<input type="checkbox"/> Group: Any Attribute: aviRole contains read-write	Tenant: All Role: From Select List System-Admin
<input type="checkbox"/> Group: Any Attribute: aviRole contains read-only	Tenant: All Role: From Select List Application-Operator

Shrubbery TAC_PLUS

- TAC_PLUS server is a much simpler alternative to ISE/ACS. This is mostly relevant in development or testing environments. Conceptually, users are assigned to groups and groups have request and response attributes.

```
key = xxxxxxxx

group = netadmin {
    default service = permit
    login = file /etc/passwd
    service = exec {
        priv-lvl = 15
    }
}

group = admin {
    default service = permit
}

group = jenkinsattrs {
    default service = permit
    service = jenkins {
        avirole = Tacacs-Admin
        avitenant = Tacacs-Tenant1
    }
}

group = jenkinsunknown {
    default service = permit
    service = jenkins {
        avirole = "Unknown Role"
        avitenant = "Unknown Tenant"
    }
}

group = jenkinsnoattrs {
    default service = permit
    service = jenkins {
    }
}

user = aviuser {
    member = netadmin
}

user = jenkinsstest1 {
    login = cleartext "password"
    member = jenkinsattrs
}

user = jenkinsstest2 {
    login = cleartext "password"
    member = jenkinsattrs
}
}
```

```
[[root@localhost ~]# cat /etc/systemd/system/tac_plus.service
[Unit]
Description=TACACS+ Service
After=syslog.target

[Service]
Type=simple
ExecStart=/usr/local/sbin/tac_plus -C /etc/tac_plus/tac_plus.conf -L -p 49 -d 65535 -Gt -l /var/log/tac_plus.log
KillMode=process
Restart=always
ExecReload=/bin/Kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

- Avi Vantage TACACS+ auth profile is configured the same way as that for ISE or ACS.

Other Articles of Interest:

[Protocol Ports Used by Avi Vantage for Management Communication](#)