



TACACS+ Configuration Examples

Avi Technical Reference (v20.1)

Copyright © 2020

TACACS+ Configuration Examples

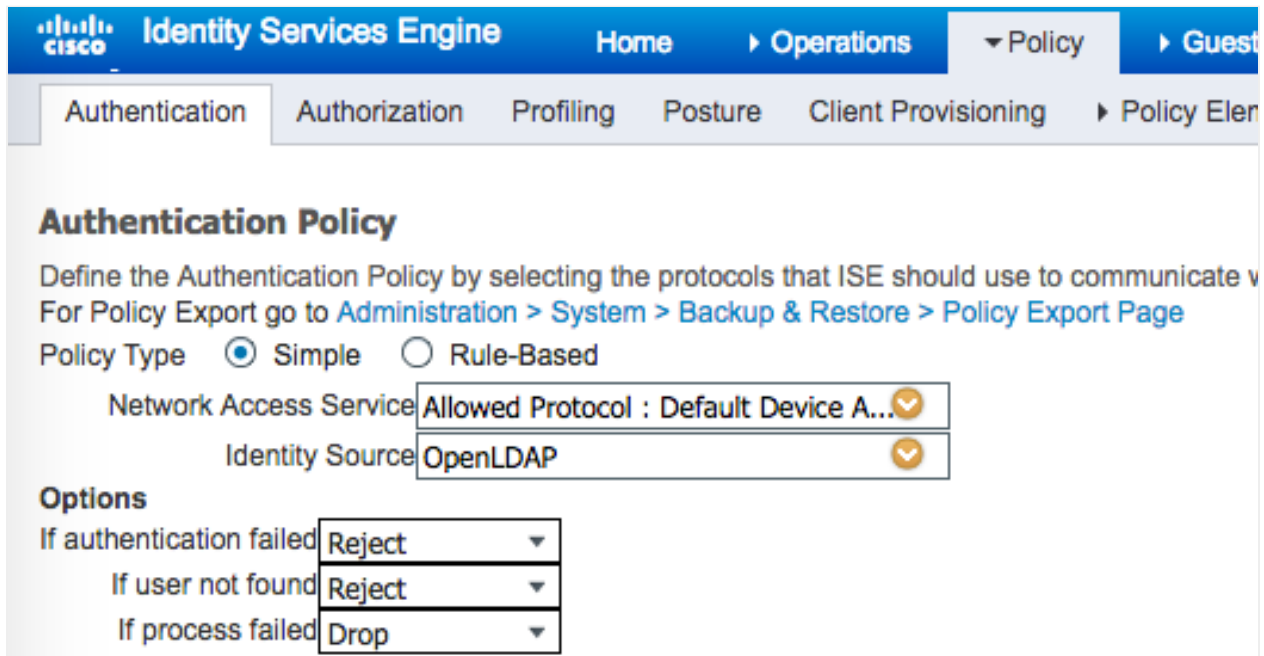
[view online](#)

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 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 folders for Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token, RSA SecurID, and SAML Id Providers. The "LDAP" folder 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

LDAP Identity Sources List > **OpenLDAP**

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes

Edit Add Delete Group

| <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

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups **Policy Conditions** Policy Results Device Admin

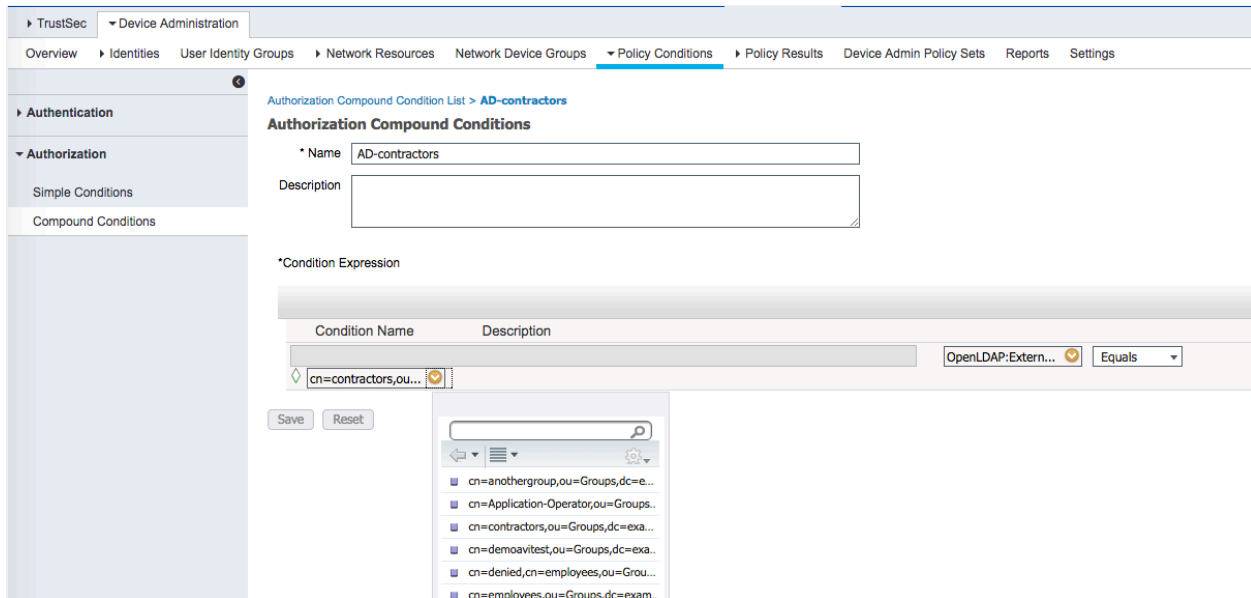
Authorization Compound Condition List >

Authorization Compound Conditions

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit Add Duplicate Delete

| <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: ⓘ

Vendor:

Supported Protocols

RADIUS

TACACS+

TrustSec

RADIUS Dictionaries:

Templates

[Expand All / Collapse All](#)

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

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 MDM

Network devices

Default Device

Network Devices List > **AviControllers**

Network Devices

* 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.

TACACS Profiles

0 Selected Rows/Page 3

Refresh Add Duplicate Trash Edit

| <input type="checkbox"/> | Name | Description |
|-------------------------------------|-----------------------|-----------------------|
| <input type="checkbox"/> | Default Shell Profile | Default Shell Profile |
| <input checked="" type="checkbox"/> | ShellProfileRO | |
| <input type="checkbox"/> | ShellProfileRW | |

TACACS Profiles > ShellProfileRW

TACACS Profile

Name * ShellProfileRW

Description

Task Attribute View Raw View

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

| | | | |
|-------------------------------------|----------------------------|--|--------------------|
| <input checked="" type="checkbox"/> | 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 to identify and authorize a Vantage user. Authorization attributes from a TACACS+ server can be used to map Avi Vantage users to various roles and tenants. In the case of an ACS server, service=avishell is required for user authorization; while in the case of an ISE server, service=avishell is known to cause authorization failure.

To know more, refer to [TACACS+ Authentication](#)

Edit Auth Profile: ISE Tacacs server

Name * ?

Type ?

LDAP
TACACS+

TACACS+ Servers ?

+ Add Item

Port ?

Password ?

TACACS+ Service ?

Login
v

TACACS+ Authorization Attributes ?

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

+ Add Attribute

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

To know more, refer to [User Account Roles](#).

Administration
Accounts
Settings
Controller
System Upgrade
GSLB
? admin (admin)

Authentication/Authorization
Access Settings
DNS / NTP
Licensing
Email/SMTP
Tenant Settings
SSH Key Settings
Upload HSM Packages

Authentication/Authorization: TACACS+

Profile: ISE Tacacs server

Tenant and Role Mapping New Mapping

Search

Displaying 2 item(s)

| Authorization | Assignment |
|---|---|
| <input type="checkbox"/> Group Any Attribute aviRole contains read-write | Tenant All Role From Select List System-Admin <div style="text-align: right; font-size: x-small;">↓ ↗</div> |
| <input type="checkbox"/> Group Any Attribute aviRole contains read-only | Tenant All Role From Select List Application-Operator <div style="text-align: right; font-size: x-small;">↑ ↗</div> |

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 = jenkinstest1 {
    login = cleartext "password"
    member = jenkinsattrs
}

user = jenkinstest2 {
    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](#)