

Configure Radius and TACACS-Based User Authentication

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Radius-Based User Authentication and Authorization for vEdge and Controllers](#)

[TACACS-Based User Authentication and Authorization for vEdge and Controllers](#)

[Related Information](#)

Introduction

This document describes how to configure Radius- and TACACS-based user authentication and authorization for vEdge and controllers with ISE.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

For the purpose of the demonstration, ISE version 2.6 is used. vEdge-cloud and controllers running 19.2.1

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, ensure that you understand the potential impact of any command.

Configure

The Viptela software provides three fixed user group names: **basic**, **netadmin**, and **operator**. You must assign the user to at least one group. The Default TACACS/Radius user is automatically placed in the basic group.

Radius-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a Viptela radius dictionary for ISE. To do so, create a text file with the content:

```
# -*- text -*-  
#
```

```

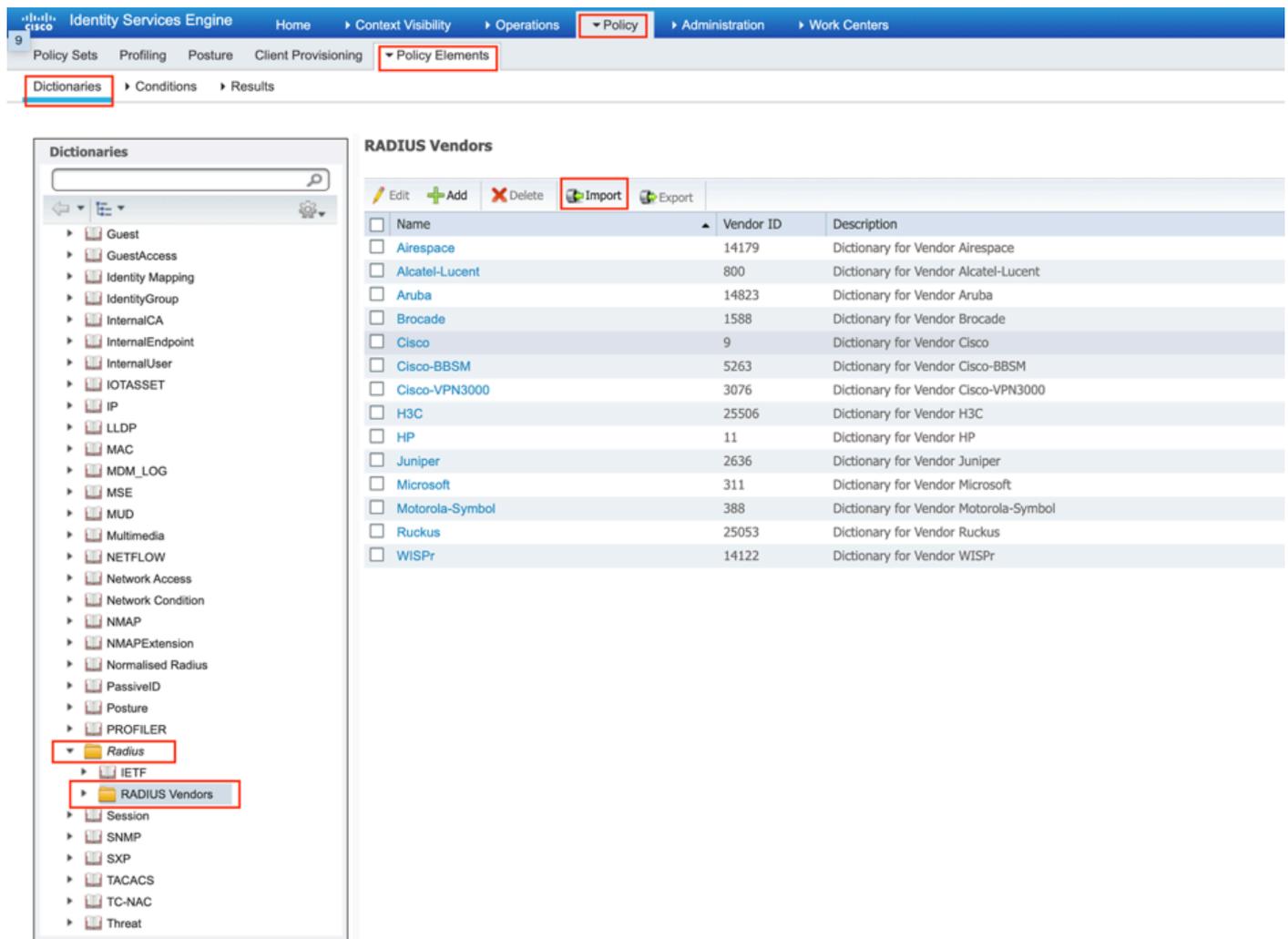
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela                41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name     1    string

```

Step 2. Upload dictionary to ISE. For this, navigate to **Policy > Policy Elements > Dictionaries**. From the list of Dictionaries, navigate to **Radius > Radius Vendors** and then click **Import** as shown.



Upload the file you created on step 1.

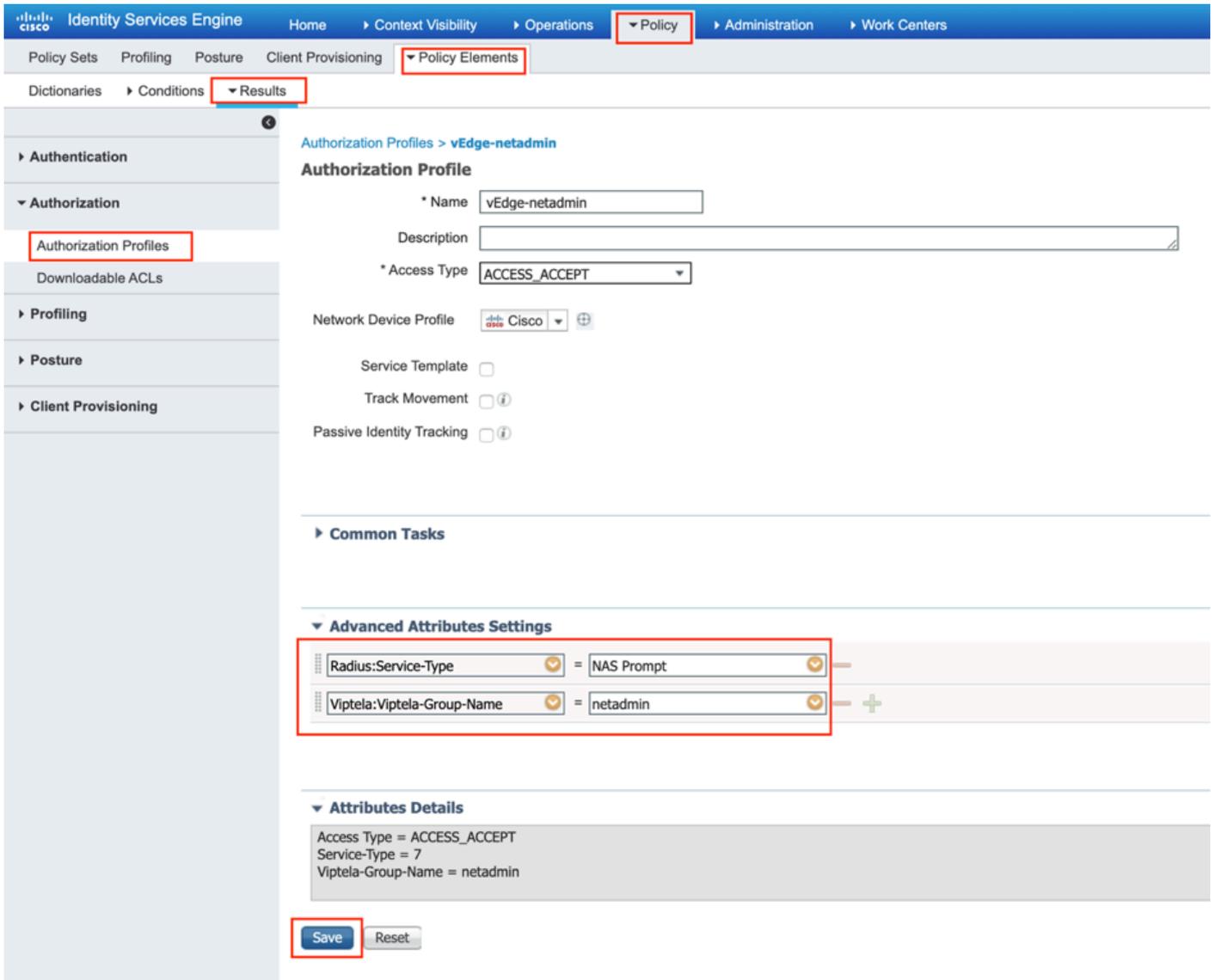
Dictionaries

Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

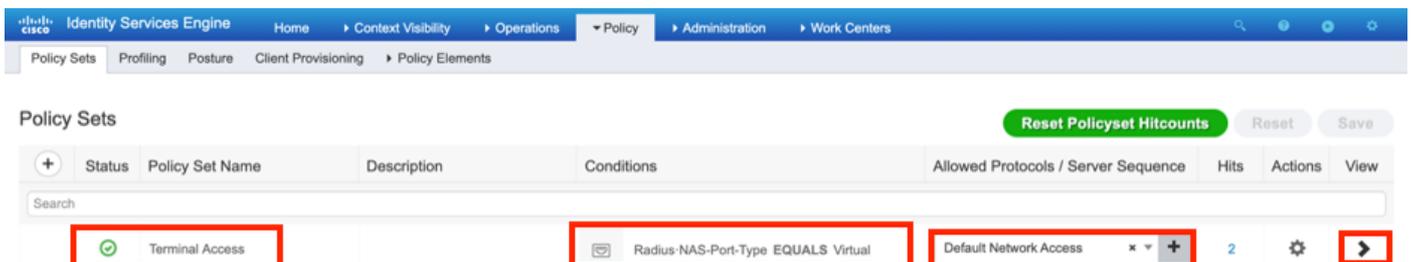
* Vendor file:

- Guest
- GuestAccess
- Identity Mapping
- IdentityGroup
- InternalCA
- InternalEndpoint
- InternalUser
- IOTASSET
- IP
- LLDP
- MAC
- MDM_LOG
- MSE
- MUD
- Multimedia
- NETFLOW
- Network Access
- Network Condition
- NMAP
- NMAPExtension
- Normalised Radius
- PassiveID
- Posture
- PROFILER
- Radius
 - IETF
 - RADIUS Vendors**
- Session
- SNMP
- SXP
- TACACS
- TC-NAC
- Threat

Step 3. Create an Authorization Profile. In this step, Radius authorization profile assigns, for example, netadmin privilege level to an authenticated user. For this, navigate to **Policy > Policy Elements > Authorization Profiles** and specify two advanced attributes as shown in the image.



Step 4. Depending on your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this article, the Policy entry called **Terminal Access** is created as shown in the image.



Click > and the next screen appears as shown in the image.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Terminal Access Reset Polycyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Terminal Access		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access x v +	2

▶ Authentication Policy (1)
 ▶ Authorization Policy - Local Exceptions
 ▶ Authorization Policy - Global Exceptions
 ▼ Authorization Policy (2)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
⋮	✓	vEdge-netadmin	IdentityGroup-Name EQUALS User Identity Groups:lab_admin	x vEdge-netadmin +	Select from list v +	1	⚙
	✓	Default		x DenyAccess +	Select from list v +	0	⚙

Reset Save

This policy matches based on user group lab_admin and assigns an authorization profile that was created in Step 3.

Step 5. Define NAS (vEdge router or controller) as shown in the image.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. Under Administration, Network Resources is selected, leading to Network Devices List > vEdge-01.

Network Devices

- * Name: vEdge-01
- Description: [Empty]
- IP Address: 10.48.87.232 / 32
- * Device Profile: Cisco
- Model Name: [Empty]
- Software Version: [Empty]
- * Network Device Group:
 - Location: All Locations (Set To Default)
 - IPSEC: No (Set To Default)
 - Device Type: All Device Types (Set To Default)

RADIUS Authentication Settings

- RADIUS UDP Settings:
 - Protocol: RADIUS
 - * Shared Secret: ***** (Show)
 - Use Second Shared Secret: [Checked] (Show)
 - CoA Port: 1700 (Set To Default)
- RADIUS DTLS Settings:
 - DTLS Required: [Checked]
 - Shared Secret: radius/dtls
 - CoA Port: 2083 (Set To Default)
 - Issuer CA of ISE Certificates for CoA: Select if required (optional)
 - DNS Name: [Empty]
- General Settings:
 - Enable KeyWrap: [Checked]
 - * Key Encryption Key: [Empty] (Show)
 - * Message Authenticator Code Key: [Empty] (Show)
 - Key Input Format: ASCII (Selected), HEXADECIMAL

Step 6. Configure vEdge/Controller.

```

system
aaa
  auth-order      radius local
  radius
  server 10.48.87.210
    vpn 512
    key cisco
  exit
!
!

```

Step 7. Verification. Log in to vEdge and ensure netadmin group assigned to the remote user.

```
vEdgeCloud1# show users
```

```
SESSION  USER      CONTEXT  FROM          PROTO  AUTH  LOGIN TIME
-----  -
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin  2020-03-09T18:39:40+00:00
```

TACACS-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a TACACS profile. In this step, the TACACS profile created is assigned, for example, netadmin privilege level to an authenticated user.

- Select **Mandatory** from the **Custom attribute** section to add the attribute as:

Type	Name	Value
Mandatory	Viptela-Group-Name	netadmin

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > vEdge

TACACS Profile

Name: vEdge_netadmin

Description:

Task Attribute View | Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege: (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape: (Select true or false)
- Timeout: Minutes (0-9999)
- Idle Time: Minutes (0-9999)

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
Mandatory	Viptela-Group-Name	netadmin

Cancel | Save

Step 2. Create a device group for SD-WAN.

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Device Groups

All Groups | Choose group

Refresh | Add | Duplicate | Edit | Trash | Show group members | Import | Export | Flat Table | Expand All | Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
SD-WAN		0
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

Description

Parent Group *

Cancel

Save

Step 3. Configure the device and assign it to the SD-WAN device group:

Network Devices List > vEdge-01

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret ⓘ

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

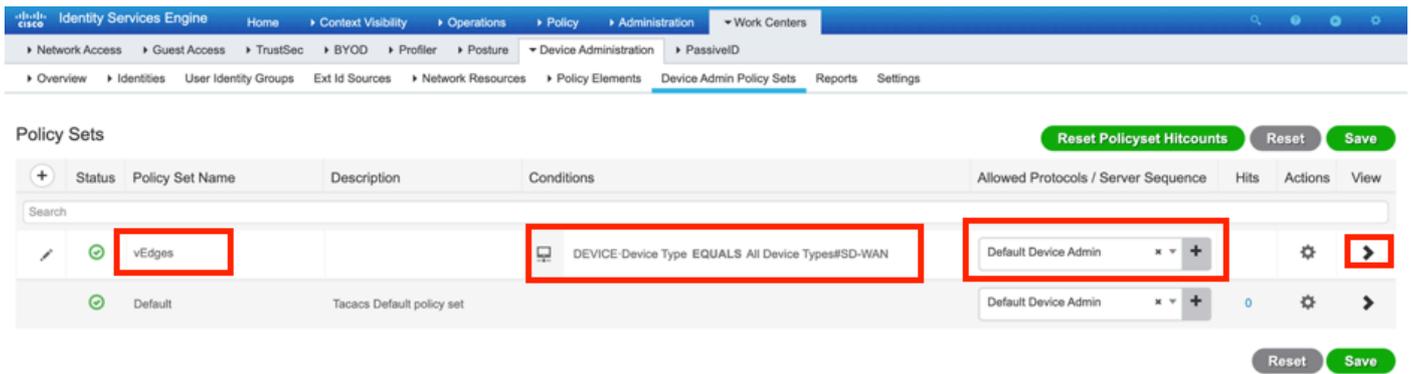
SNMP Settings

Advanced TrustSec Settings

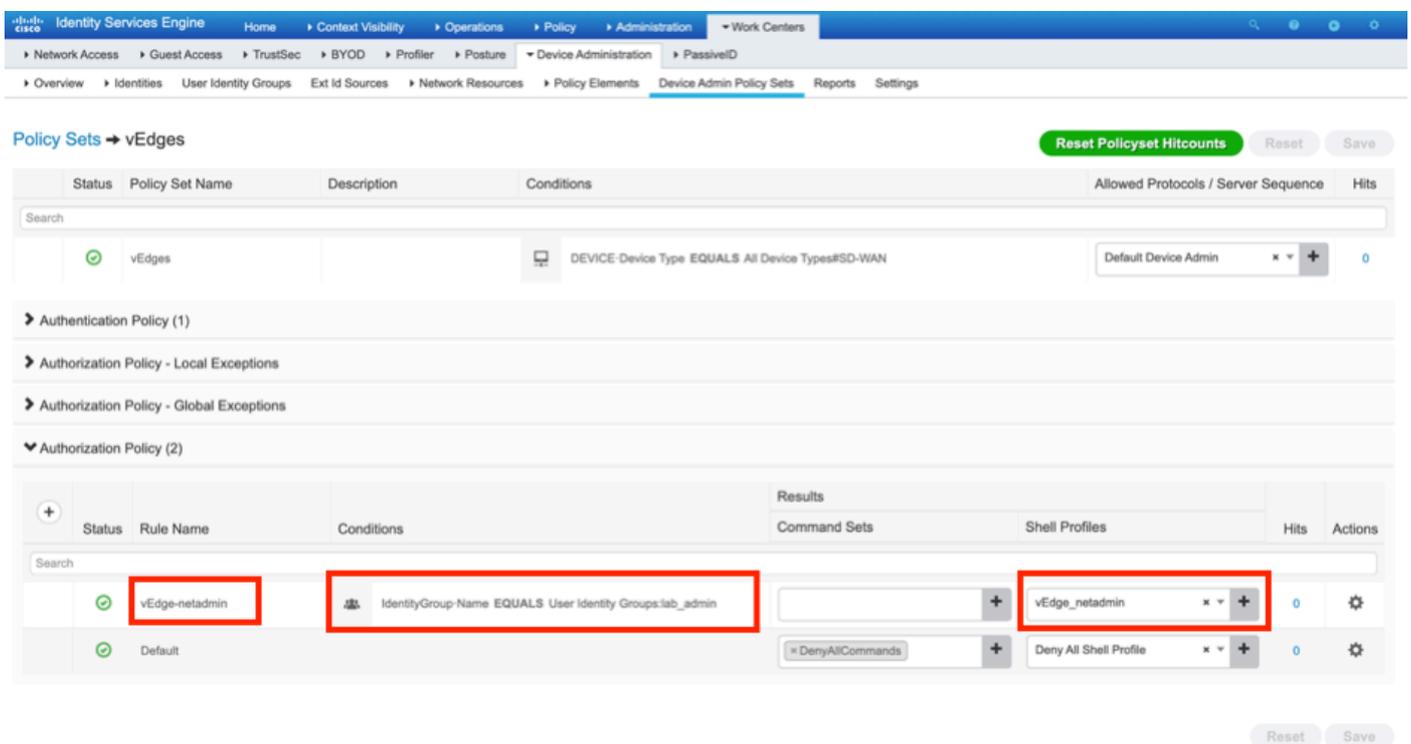
Save

Step 4. Define Device Administration Policy.

Depending on your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this document, the Policy is created.



Click > and the next screen appears as shown in this image. This policy matches based on device type named **SD-WAN** and assigns the Shell profile that is created in step 1.



Step 5. Configure vEdge:

```

system
aaa
  auth-order tacacs local
  !
tacacs
  server 10.48.87.210
    vpn 512
    key cisco
  exit
  !
!

```

Step 6. Verification. Login to vEdge and ensure netadmin group assigned to remote user:

```
vEdgeCloud1# show users
```

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

Related Information

- **Cisco ISE Device Administration Prescriptive Deployment Guide:** <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- **Configuring User Access and Authentication:**