Use LDAP for End User Authentication

For supported software information, click here.

Authentication is a mechanism for verifying the identities of users so that only genuine users have access to applications. You can choose from various authentication methods to authenticate end-use s through a captive portal and an authenticate firewall. You can configure either a user-based or group-based policy to set whether to allow or deny traffic.

On Versa Operating System^{TM} (VOS^{TM}) devices, you can configure a number of authentication methods to authenticate end users, including using a local database, using a Lightweight Directory Access Protocol (LDAP) server, Security Assertion Markup Language (SAML), and Kerberos. This article describes how to configure an LDAP server to use for end user authentication.

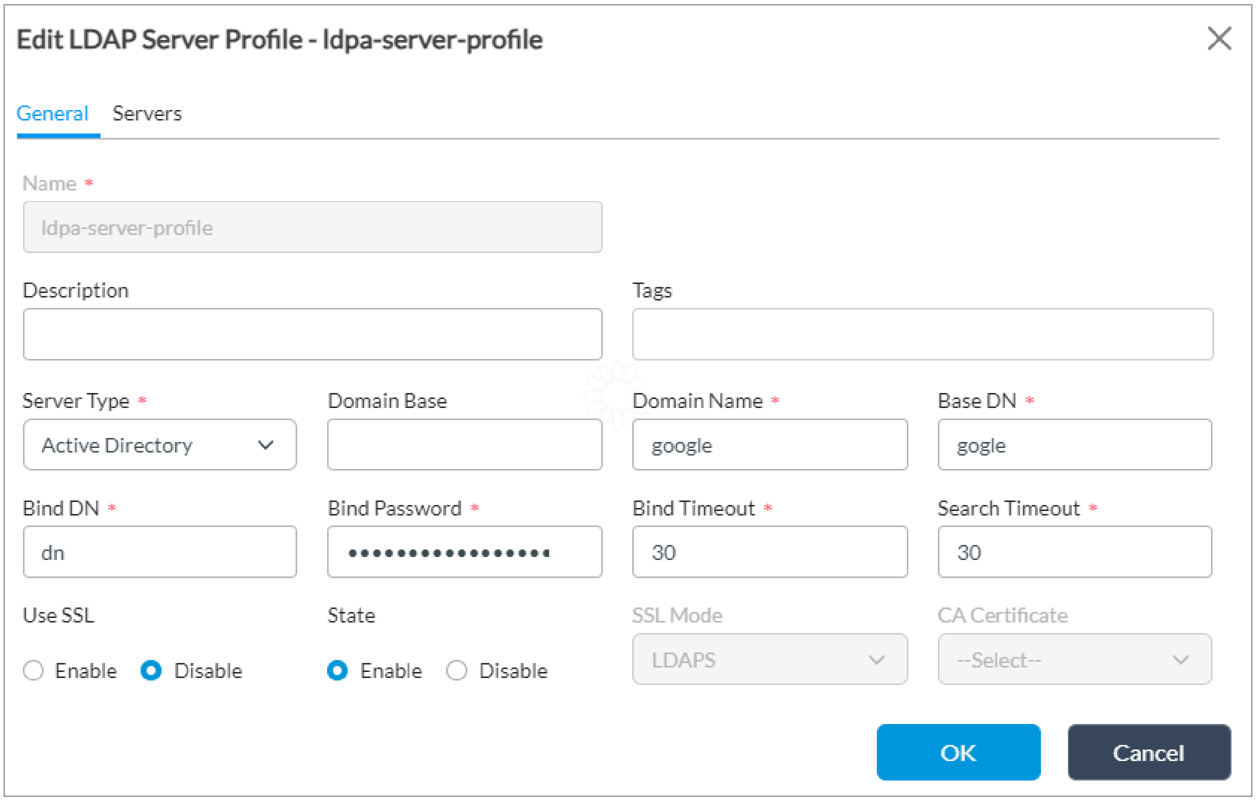
LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information. When an end user sends a request to access a webpage, the VOS device accesses the LDAP server to validate the user. Based on the authentication result, the user is either authentication or their authentication request is denied. You can configure either a user-based or group-based policy to allow or deny traffic.

For LDAP authentication to work, you must enable the NGFW service on the VOS device. For more information, see Configure NGFW.

Configure LDAP for End User Authentication

To authenticate users using LDAP and an LDAP server:

1. Configure an LDAP server profile. Currently, the LDAP server type can only be Active Directory. For configuration information, see Configure an LDAP Server Profile.

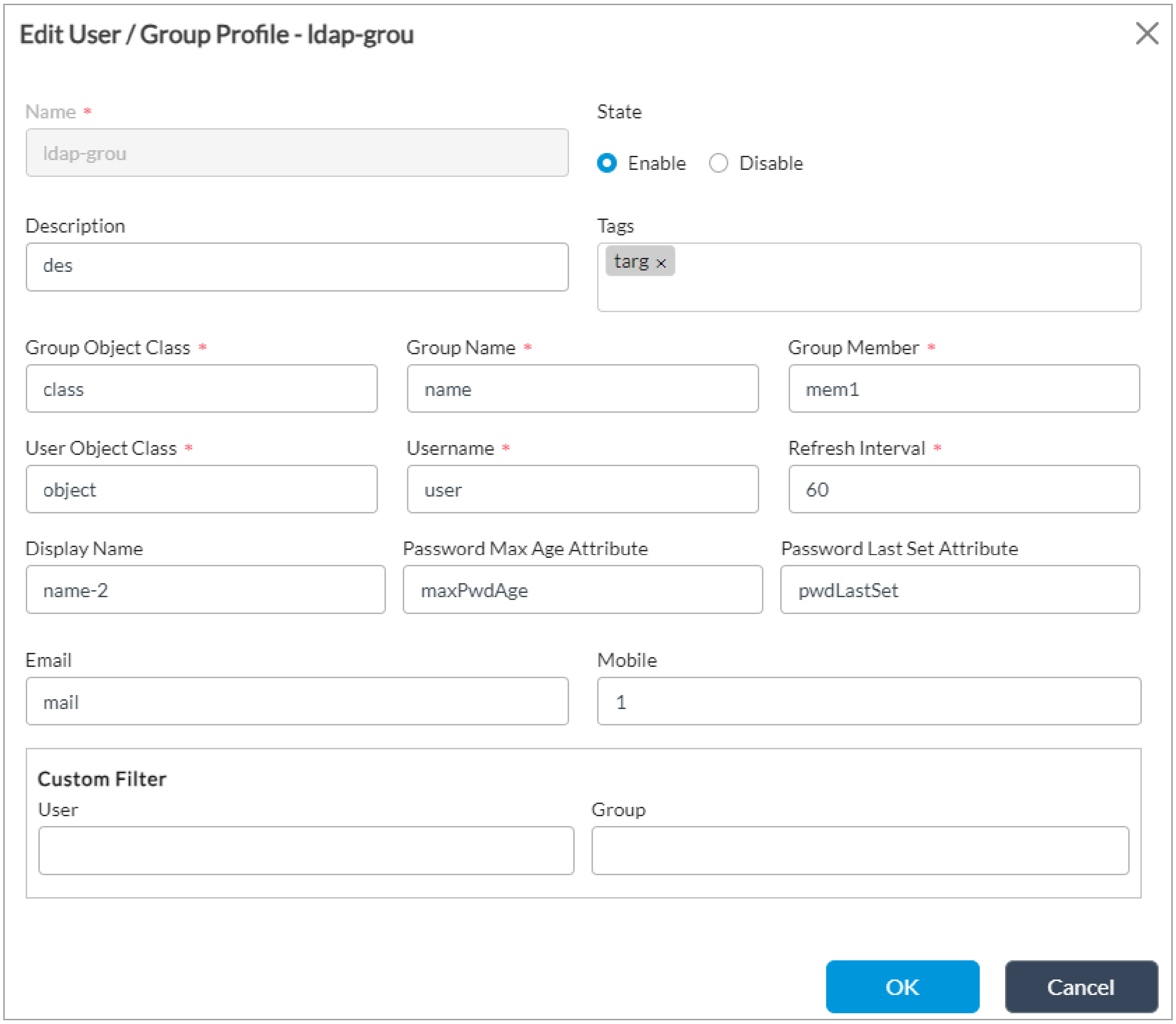


Edit LDAP Server Profile - ldpa-server-profile

General Servers

Name *			
ldpa-server-profile			
Description		Tags	
Server Type *	Domain Base	Domain Name *	Base DN *
Active Directory		google	gogle
Bind DN *	Bind Password *	Bind Timeout *	Search Timeout *
dn	•••••••••••••••••	30	30
Use SSL	State	SSL Mode	CA Certificate
○ Enable ● Disable	● Enable ○ Disable	LDAPS	--Select--

2. Configure an LDAP user group profile. For configuration information, see Configure a User and Group Mapping Profile.



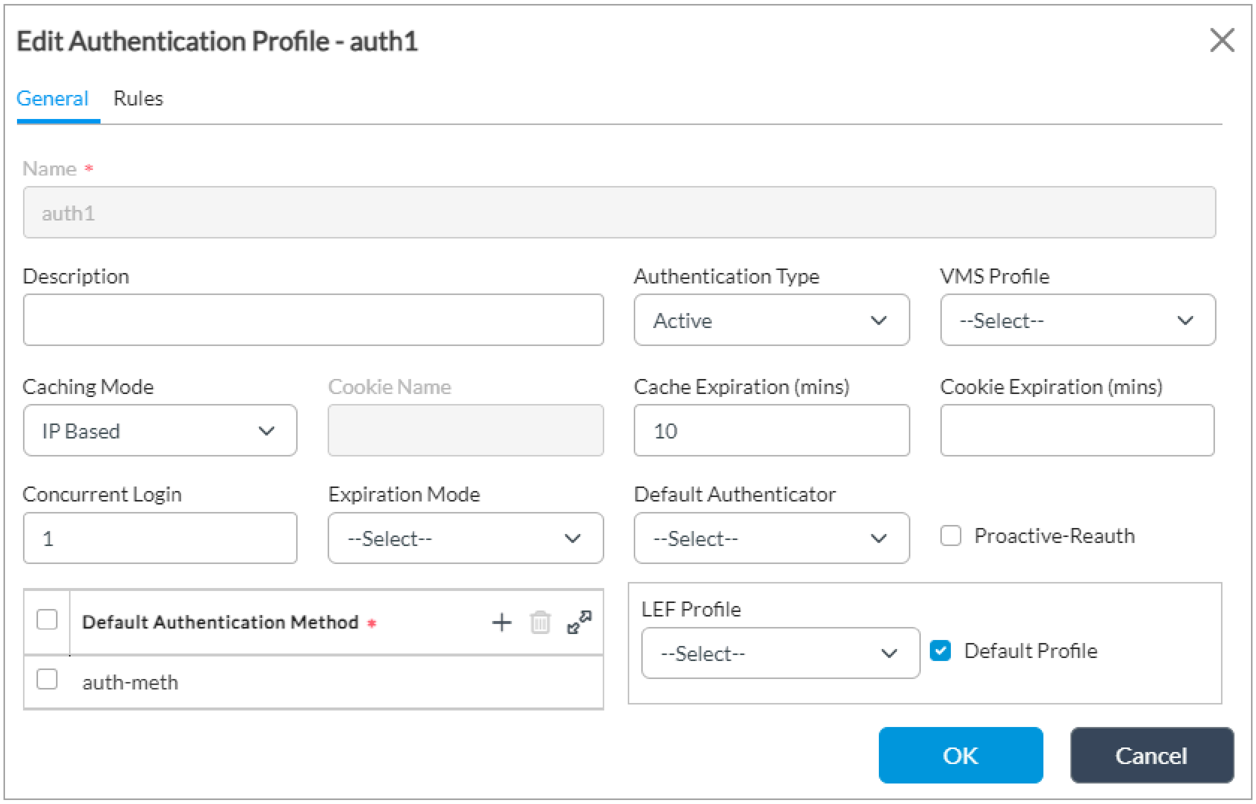
Edit User / Group Profile - ldap-grou

Name *	ldap-grou
State	● Enable ○ Disable
Description	des
Tags	targ ×
Group Object Class *	class
Group Name *	name
Group Member *	mem1
User Object Class *	object
Username *	user
Refresh Interval *	60
Display Name	name-2
Password Max Age Attribute	maxPwdAge
Password Last Set Attribute	pwdLastSet
Email	mail
Mobile	1

Custom Filter

User	
Group	

3. Create an authentication profile in which you associate the LDAP authentication profile you created in Step 1. For configuration information, see Configure an Authentication Profile. If you create an authentication profile without creating an LDAP profile, you must create an LDAP profile here.



Edit Authentication Profile - auth1

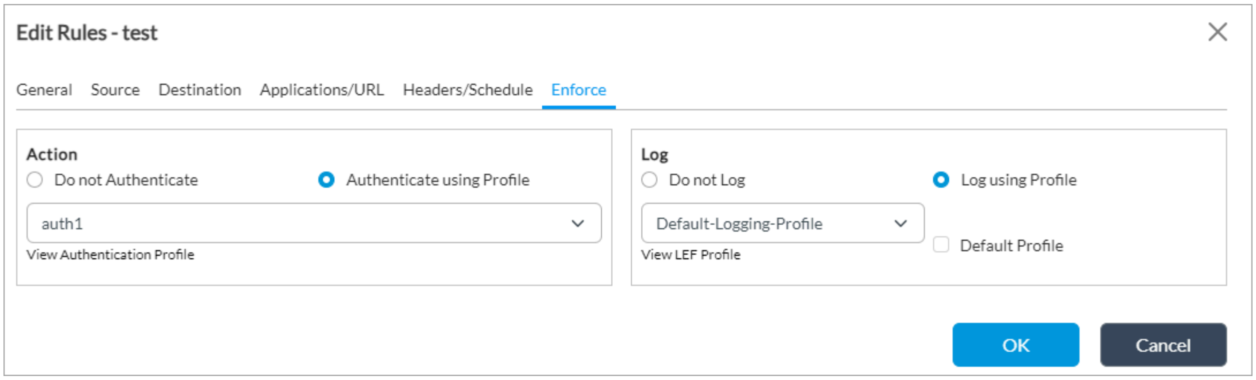
General | Rules

Name * auth1			
Description		Authentication Type: Active	VMS Profile: --Select--
Caching Mode: IP Based	Cookie Name	Cache Expiration (mins): 10	Cookie Expiration (mins)
Concurrent Login: 1	Expiration Mode: --Select--	Default Authenticator: --Select--	□ Proactive-Reauth

□	Default Authentication Method *
□	auth-meth

LEF Profile: --Select-- ☑ Default Profile

4. Create an authentication rule in which you select the authentication profile you created in Step 3 to use for the enforcement action. For more information, see Configure Rules for Authentication Policies.



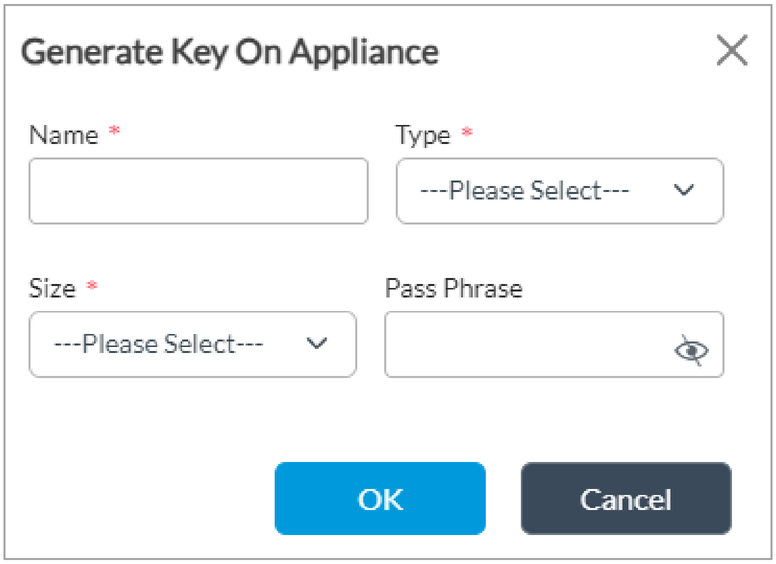
Edit Rules - test

General | Source | Destination | Applications/URL | Headers/Schedule | Enforce

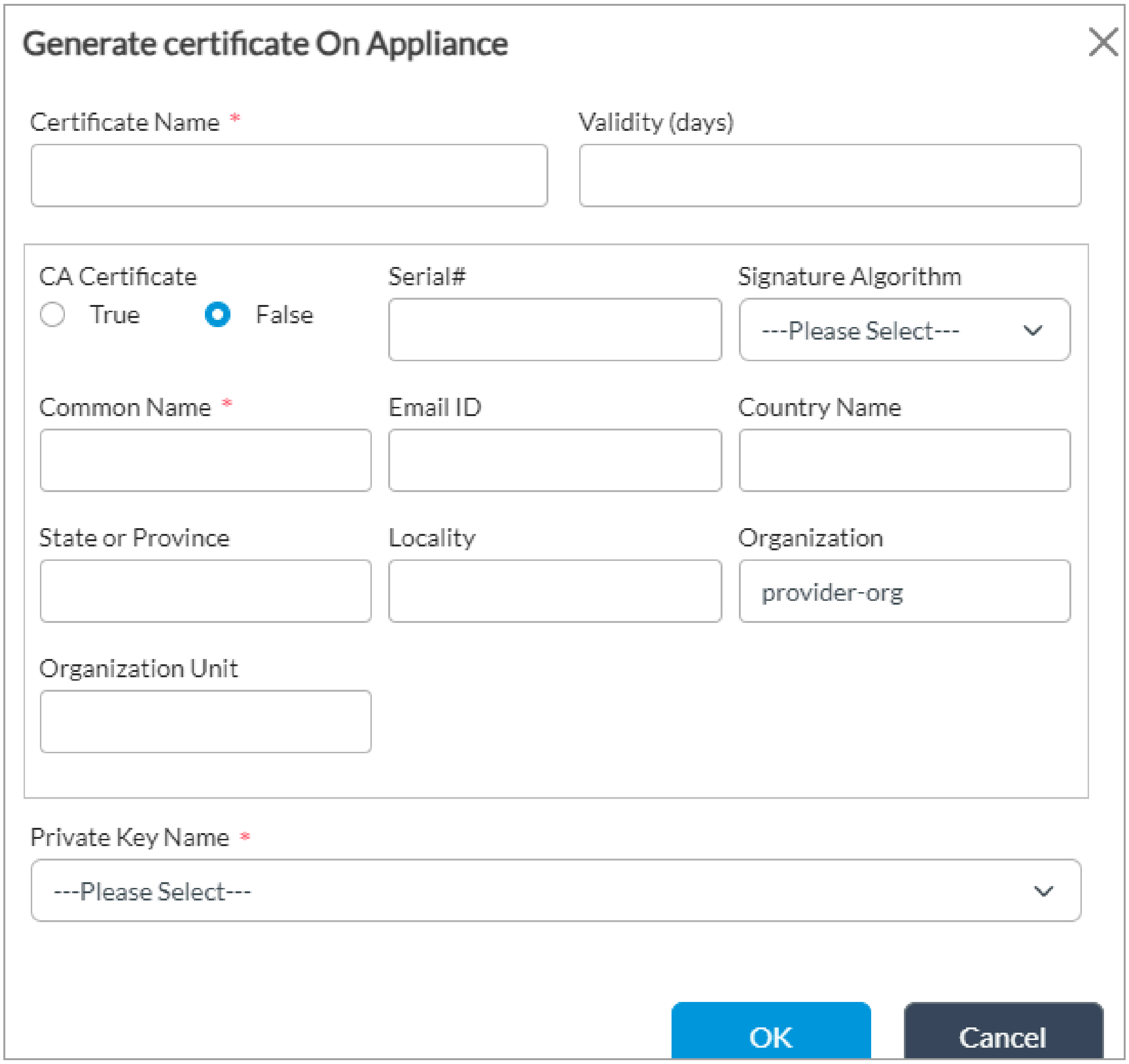
Action
○ Do not Authenticate ● Authenticate using Profile
auth1
View Authentication Profile

Log
○ Do not Log ● Log using Profile
Default-Logging-Profile □ Default Profile
View LEF Profile

5. Configure the captive portal:
   a. Create a private key for the certificate. This is required because the captive portal uses a self-signed certificate. For more information, see Create a CA Certificate Key.



b. Create the certificate and assign the private key you generated in Step 5a. For more information, see [Create a Certificate on a VOS Device]().

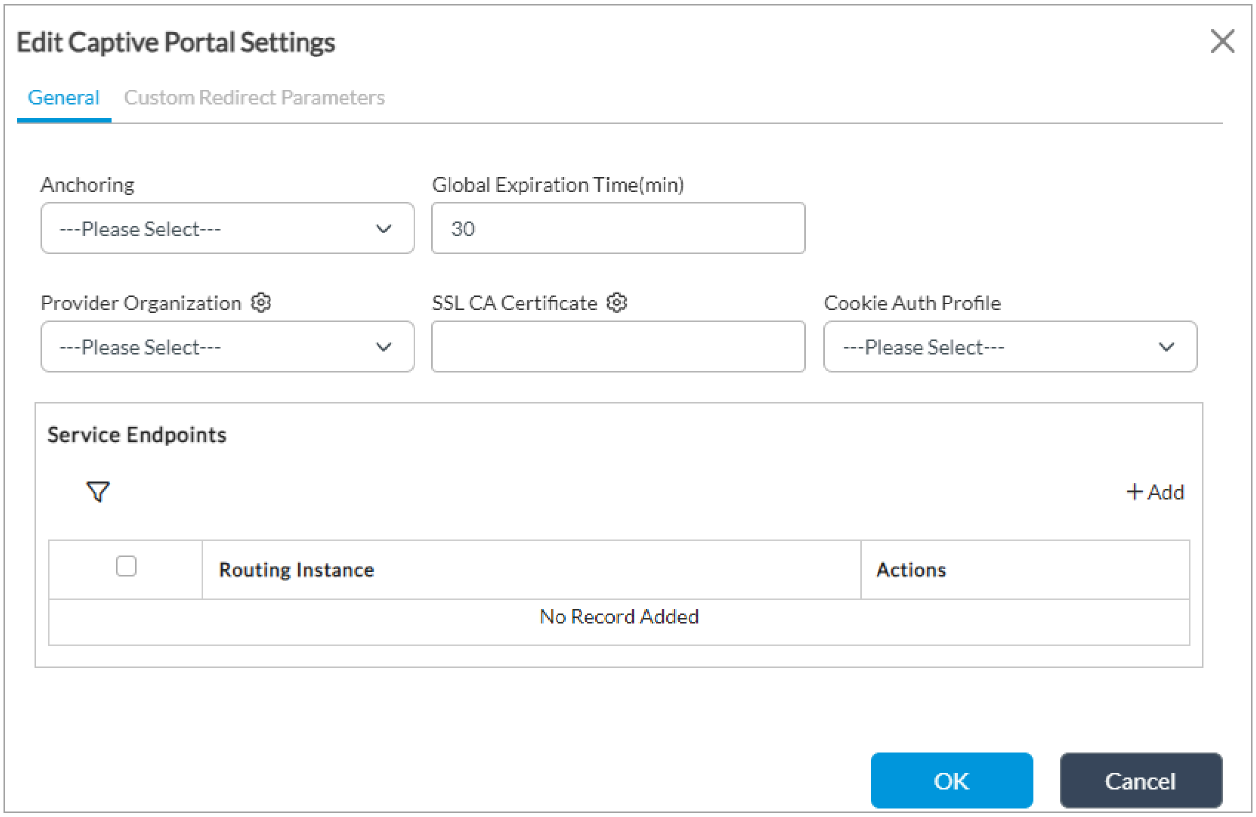


Generate certificate On Appliance

CA Certificate ○ True ● False

Organization: provider-org

c. Configure the captive portal. For more information, see Configure Captive Portal.



Edit Captive Portal Settings

Anchoring: ---Please Select---

Global Expiration Time(min): 30

Provider Organization: ---Please Select---

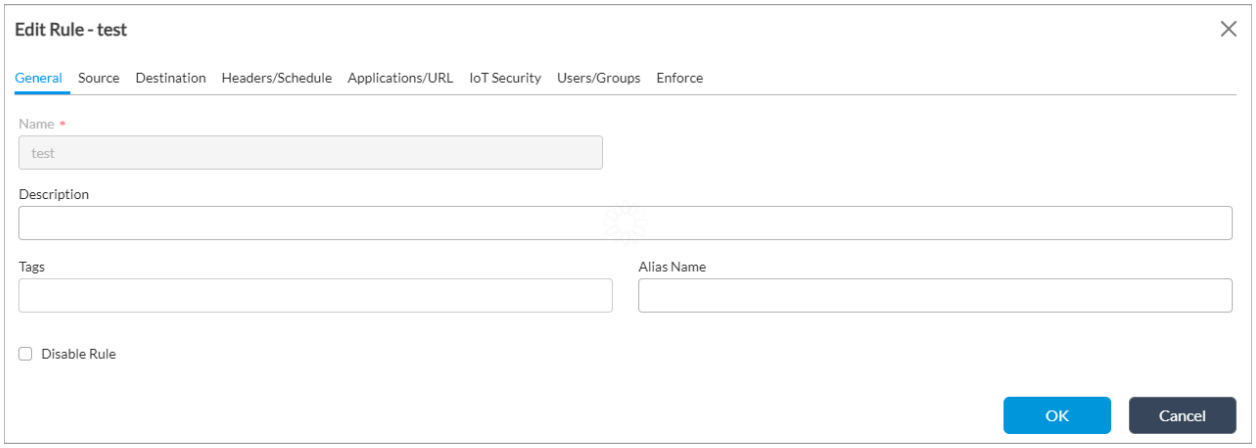
SSL CA Certificate:

Cookie Auth Profile: ---Please Select---

Service Endpoints

□	Routing Instance	Actions
No Record Added		

6. Create an access policy rule to allow the traffic you want to authenticate. For more information, see [Configure Access Policy Rules]().



Edit Rule - test

Name *: test

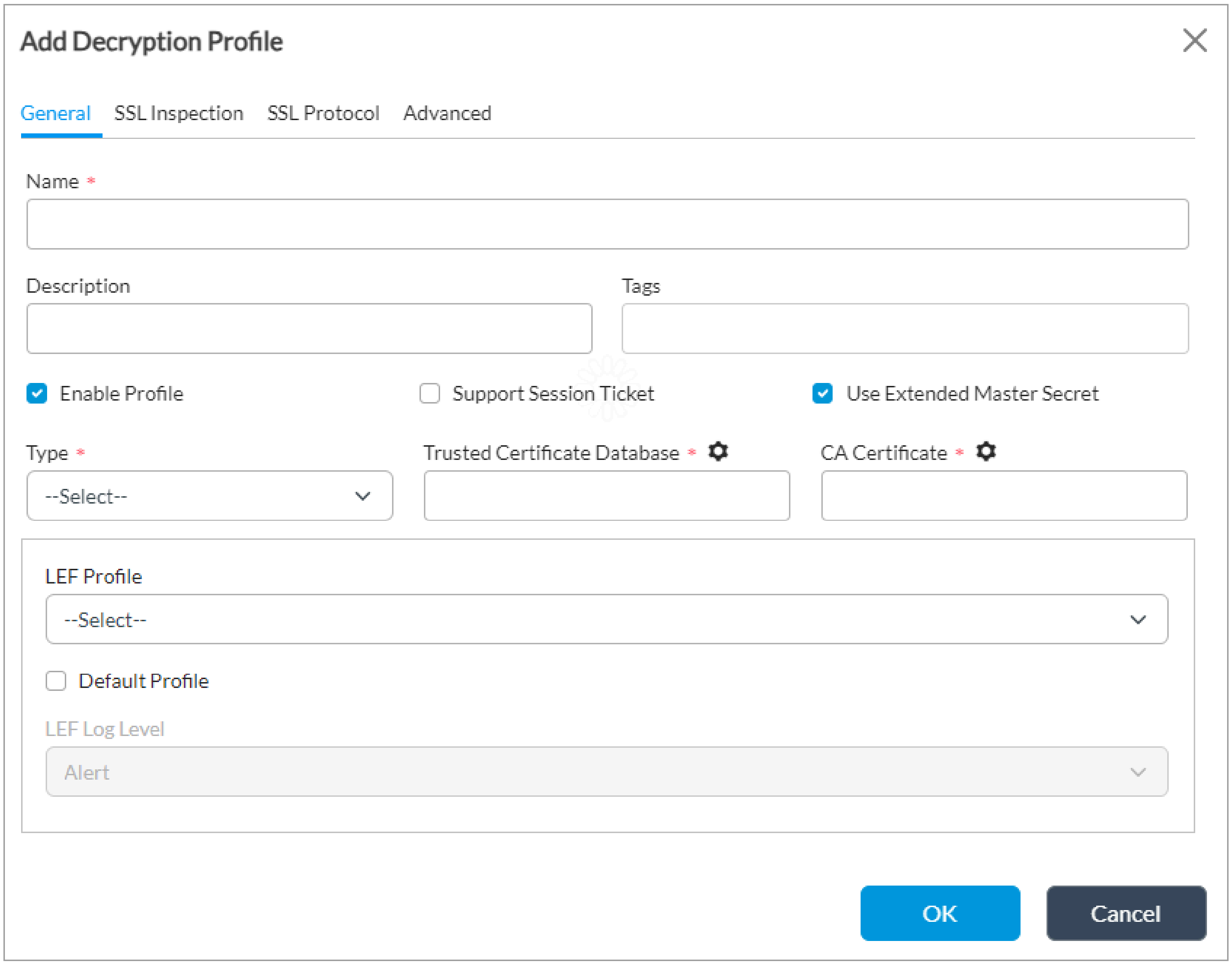
Description:

Tags:

Alias Name:

□ Disable Rule

7. If you are authenticating HTTPS traffic, configure an SSL decryption profile. For more information, see [Configure an SSL Decryption Profile]().



Add Decryption Profile

General | SSL Inspection | SSL Protocol | Advanced

Name *

Description

Tags

☑ Enable Profile

□ Support Session Ticket

☑ Use Extended Master Secret

Type * --Select--

Trusted Certificate Database *

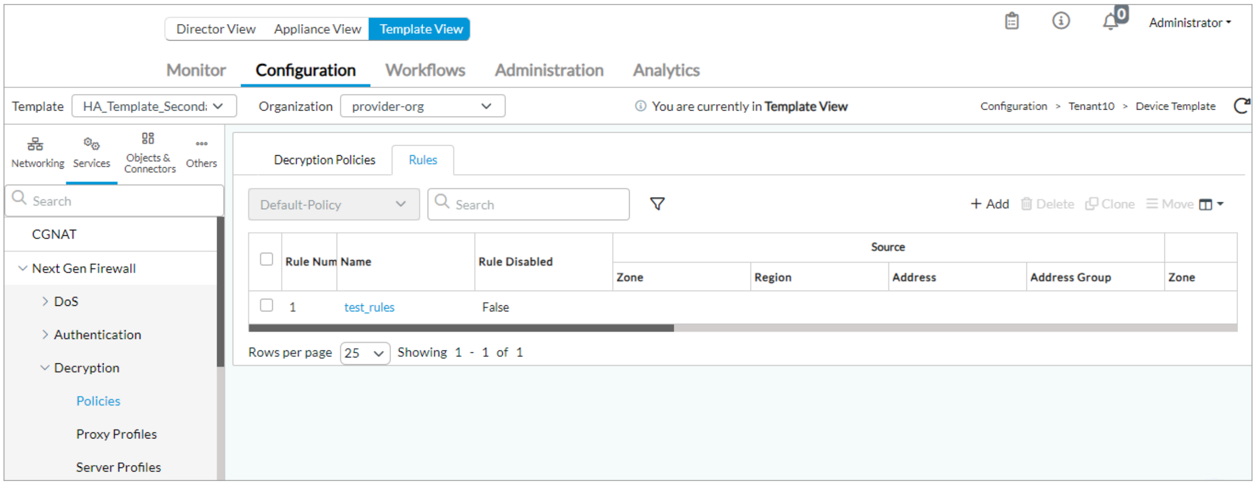
CA Certificate *

LEF Profile --Select--

□ Default Profile

LEF Log Level Alert

8. If you are authenticating HTTPS traffic, configure an SSL decryption policy that sets the decrypt action. For more information, see Configure an SSL Decryption Profile.



Template HA_Template_Second:

Organization provider-org

You are currently in **Template View**

Configuration > Tenant10 > Device Template

Default-Policy

□	Rule Num	Name	Rule Disabled	Source				
				Zone	Region	Address	Address Group	Zone
□	1	test_rules	False					

Rows per page 25 Showing 1 - 1 of 1

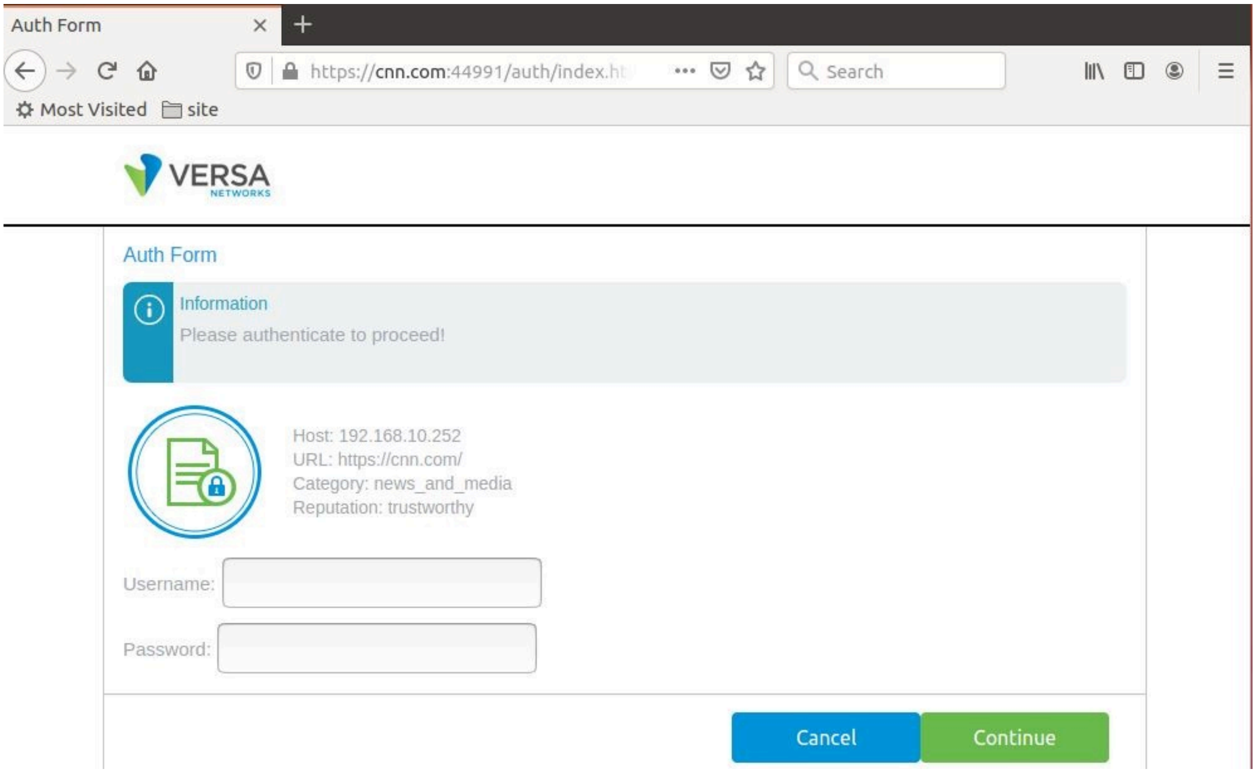
9. Export the self-signed certificate, and then import it to the Windows computer.

For information about how to match a specific user from LDAP, see Add External Database Users in Configure User and Group Policy.

Use Case Example

This section shows an example of how the LDAP configuration authenticates end users.

1. An unauthenticated user enters a webpage address in the URL. A captive portal window similar to the following displays:



Auth Form

Information

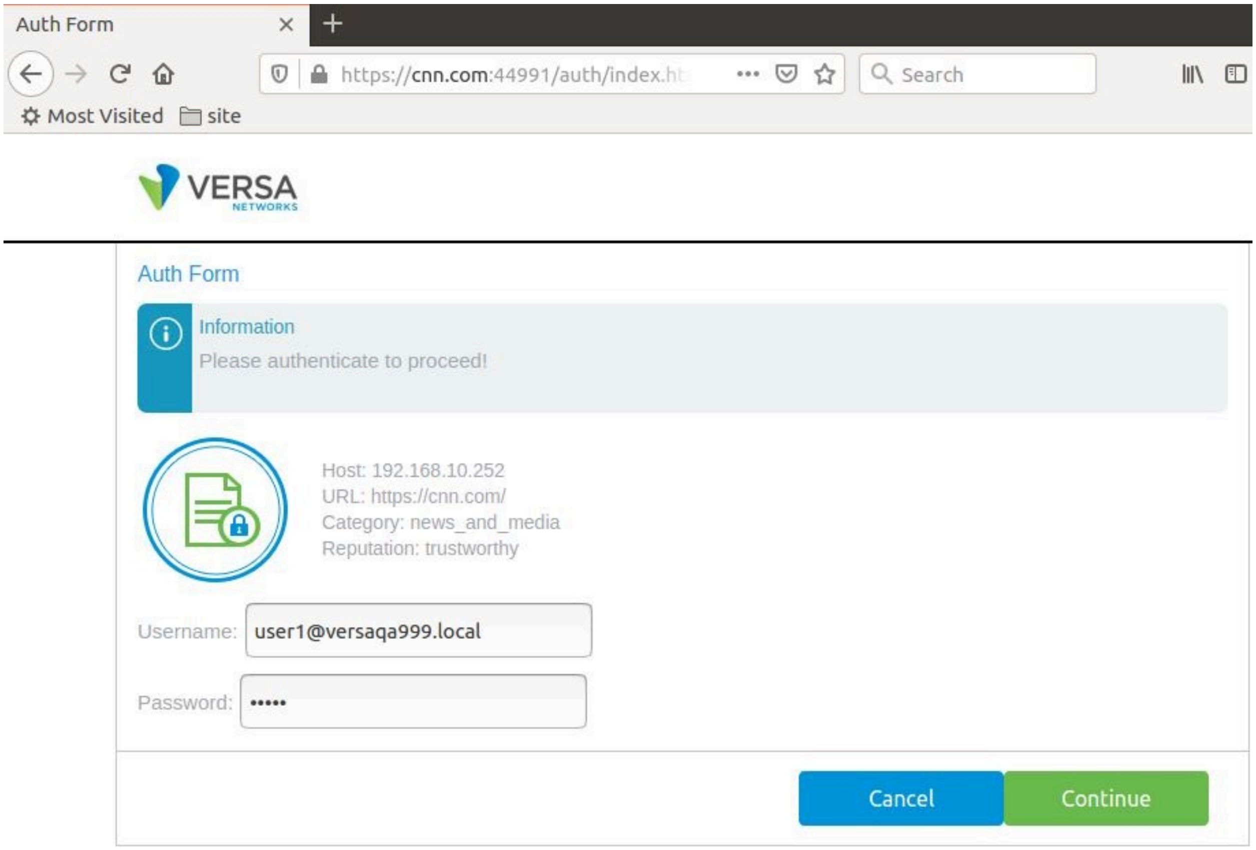
Please authenticate to proceed!

Host: 192.168.10.252
URL: https://cnn.com/
Category: news_and_media
Reputation: trustworthy

Username:

Password:

2. The user enters their credentials and then clicks Continue.


Auth Form

https://cnn.com:44991/auth/index.ht

Auth Form

Information

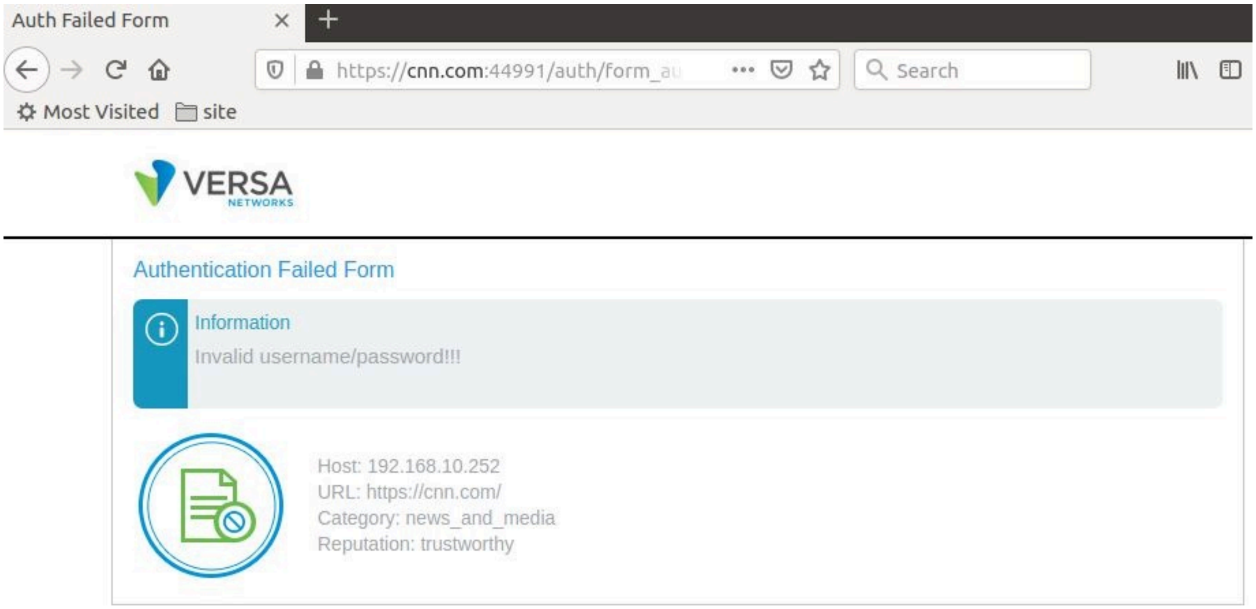
Please authenticate to proceed!

Host: 192.168.10.252
URL: https://cnn.com/
Category: news_and_media
Reputation: trustworthy

Username: user1@versaqa999.local

Password: •••••

a. If the credentials are correct based on the LDAP configuration, the webpage opens successfully.
b. If the credentials are incorrect based on the LDAP configuration, a window similar to the following displays:


Auth Failed Form

https://cnn.com:44991/auth/form_au

Authentication Failed Form

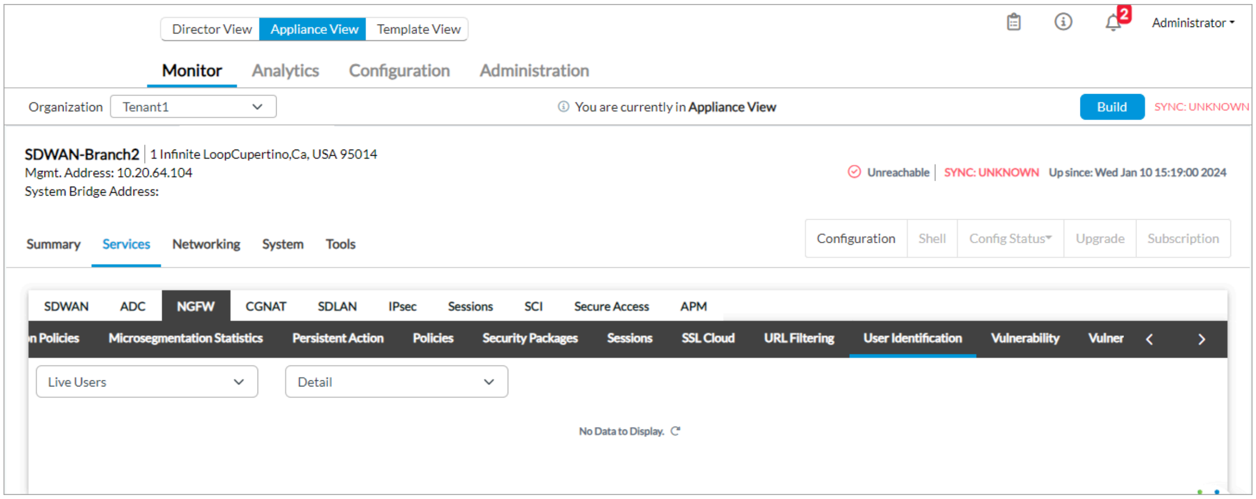
Information

Invalid username/password!!!

Host: 192.168.10.252
URL: https://cnn.com/
Category: news_and_media
Reputation: trustworthy

3. To view profile statistics for custom profiles:
   a. In Appliance view, select the Monitor tab in the top menu bar.

b. Select the Services tab in the horizontal menu bar.
c. Select NGFW > User Identification.
d. Select Live Users in the drop-down menu. The window displays statistics for the currently active users.



Organization Tenant1

You are currently in Appliance View

SYNC: UNKNOWN

SDWAN-Branch2 | 1 Infinite LoopCupertino,Ca, USA 95014
Mgmt. Address: 10.20.64.104
System Bridge Address:

Unreachable | SYNC: UNKNOWN Up since: Wed Jan 10 15:19:00 2024

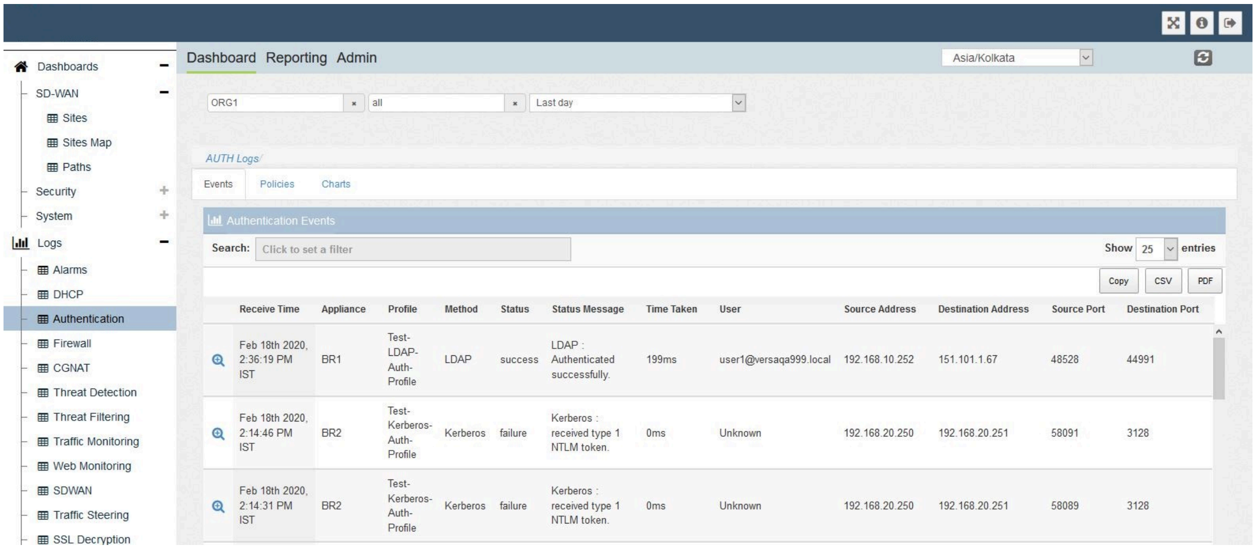
Live Users

Detail

No Data to Display.

4. To view the authentication logs on the Analytics node:

a. Log in to the Analytics node that is integrated with the Director node.
b. Select the Dashboard tab in the top menu bar.
c. Select Logs > Authentication in the left navigation bar. The following window displays, showing the logs panes with top data.



Asia/Kolkata

ORG1 | all | Last day

AUTH Logs

Authentication Events

Search: Click to set a filter

Show 25 entries

Receive Time	Appliance	Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port	Destination Port
Feb 18th 2020, 2:36:19 PM IST	BR1	Test-LDAP-Auth-Profile	LDAP	success	LDAP : Authenticated successfully.	199ms	user1@versaqa999.local	192.168.10.252	151.101.1.67	48528	44991
Feb 18th 2020, 2:14:46 PM IST	BR2	Test-Kerberos-Auth-Profile	Kerberos	failure	Kerberos : received type 1 NTLM token.	0ms	Unknown	192.168.20.250	192.168.20.251	58091	3128
Feb 18th 2020, 2:14:31 PM IST	BR2	Test-Kerberos-Auth-Profile	Kerberos	failure	Kerberos : received type 1 NTLM token.	0ms	Unknown	192.168.20.250	192.168.20.251	58089	3128

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure HTTP/HTTPS Proxy
Configure Kerberos Authentication
Configure NGFW
Configure URL Filtering
Configure User and Group Policy