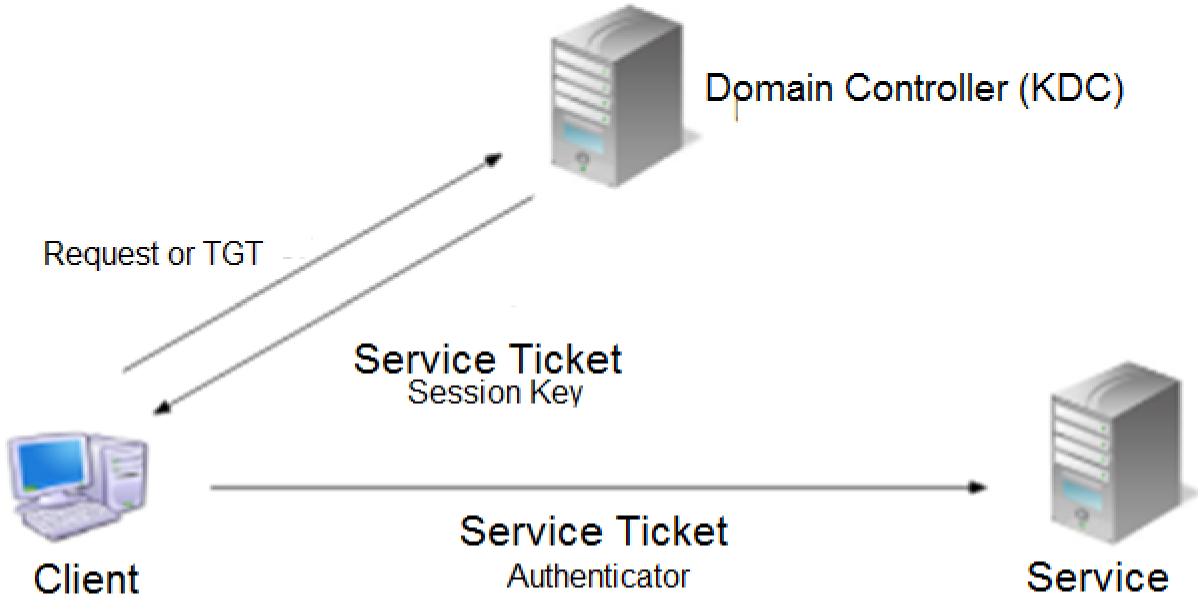
Configure Kerberos Authentication

For supported software information, click here.

You can configure Kerberos authentication on Versa Operating System^{TM} (VOS^{TM}) devices. Kerberos provides strong authentication for users and groups, and its authentication is stronger than LDAP. Kerberos uses secret key cryptography, so it never transmits user credentials over the network.

The following figure illustrates how Kerberos authentication works. The client, here, the VOS device, authenticates itself using the authentication server, and the authentication server forwards the username to the key distribution center (KDC). The KDC issues a ticket-granting ticket (TGT), which includes a timestamp, encrypts the TGT using the ticket-granting service (TGS) secret key, and returns the encrypted TGT to the user. The user verifies the validity of the TGT and is then granted access to the requested service. The TGS issues a service ticket and a session key to the client. The client then sends the service ticket, along with its service request, to the service server.



To configure Kerberos authentication, you do the following:

1. Generate and upload the keytab file.
2. Configure a Kerberos profile.

3. Configure an authentication profile for Kerberos.
4. Create an authentication rule for Kerberos.
5. Configure captive portal.
6. Configure a decryption profile with full proxy (transparent or explicit proxy).
7. Configure a decryption rule.
8. Configure secure web proxy (transparent or explicit proxy)
9. Configure browser settings for Kerberos.

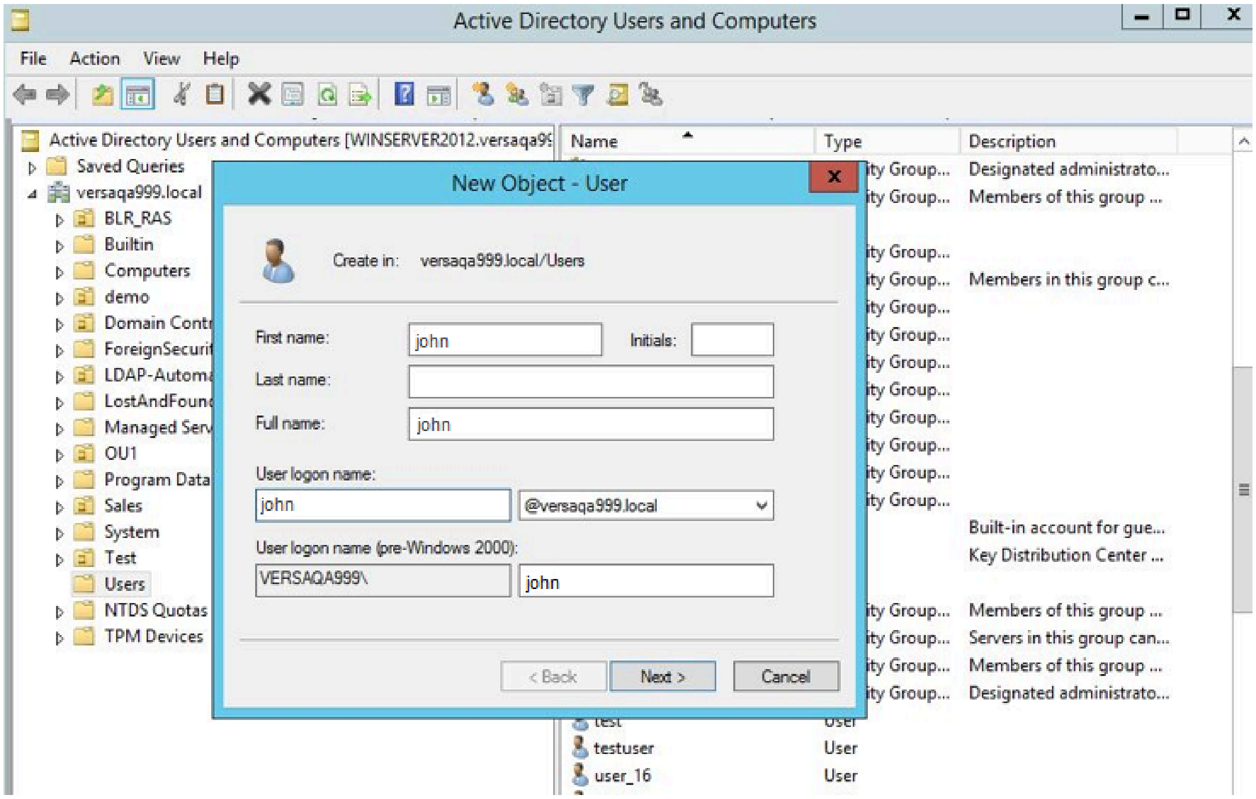
Configure Kerberos Keytabs

To use Kerberos, you generate a keytab file and then upload it to one or more VOS devices. You use the Kerberos keytab file to authenticate systems and services that use Kerberos without having to enter a password.

Note that because the keytabs are derived from the Kerberos password, if you change the Kerberos password, you must re-create all keytabs and import the keytab files to the device again.

Generate a Keytab File on an Active Directory Server

1. Create a domain user on the Active Directory (AD) server:



New Object - User

Create in: versaqa999.local/Users

First name: john
Initials:
Last name:
Full name: john
User logon name: john @versaqa999.local
User logon name (pre-Windows 2000): VERSAQA999\ john

2. On the Active Directory server, log in to Windows PowerShell (command-line shell) and generate the keytab file.

```
ktpass.exe -princ spn L -mapuser username -mapOp set -pass password -crypto all -ptype KRB5_NT_
PRINCIPAL -out filename.keytab
```

In this command:

- princ HTTP/john.versaqa999.local@VERSAQA999.LOCAL—Enter the service principal name, in the format of *user@realm*.
- mapuser *username*—Enter the username.
- –pass *password*—Enter the user password.
- –out *filename*.keytab—Enter the name of the file in which to save the keytabs.

For example:

```
ktpass.exe -princ HTTP/john.versaqa999.local@VERSAQA999.LOCAL -mapuser john -mapOp set -
pass Versa@123 -crypto all -ptype KRB5_NT_PRINCIPAL -out Sample.keytab
```

Use a Keytab File on Multiple Devices

To use the same keytab file on multiple VOS devices and to configure different virtual URLs in captive portal, you must configure multiple service principal names (SPN) in the user account. The user account is the domain user account that is used to generate the keytab file.

Note: Use this procedure only if you are configuring the same keytab file on multiple devices.

To configure multiple SPNs:

1. Log in to Windows PowerShell.
2. Configure the SPN directory property for the AD service account:

```
setspn.exe -S HTTP/spn-name username
setspn.exe -S HTTP/spn-name2 username
```

For example:

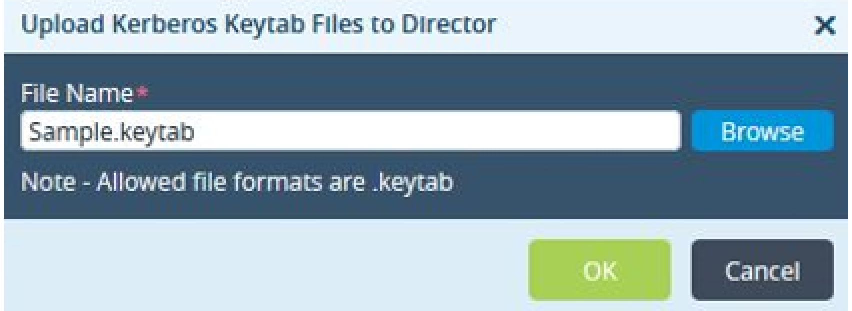
```
PS C:\Users\Administrator.WINSERVER> setspn -S HTTP/br1.versaqa999.local john
Checking domain DC=spn999,DC=local

Registering ServicePrincipalNames for CN=john,CN=Users,DC=versaqa999,DC=local
        HTTP/br1.versaqa999.local
Updated object

PS C:\Users\Administrator.WINSERVER> setspn -S HTTP/br2.versaqa999.local john
Checking domain DC=versaqa999,DC=local

Registering ServicePrincipalNames for CN=john,CN=Users,DC=versaqa999,DC=local
        HTTP/br2.versaqa999.local
Updated object
```

3. Verify the SPN by issuing the **setspn –l** *username* command. For example:

```
PS C:\Users\Administrator.WINSERVER> setspn -l john
Registered ServicePrincipalNames for CN=john,CN=Users,DC=versaqa999,DC=local:
        HTTP/br2.versaqa999.local
        HTTP/br1.versaqa999.local
        HTTP/john.versaqa999.local
```

Upload the Kerberos Keytab File

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Kerberos Keytab in the left menu bar.
4. Select the Director tab, and then click the Upload icon to upload the keytab file to the Director node. The Upload Kerberos Keytab Files to Director popup window displays.



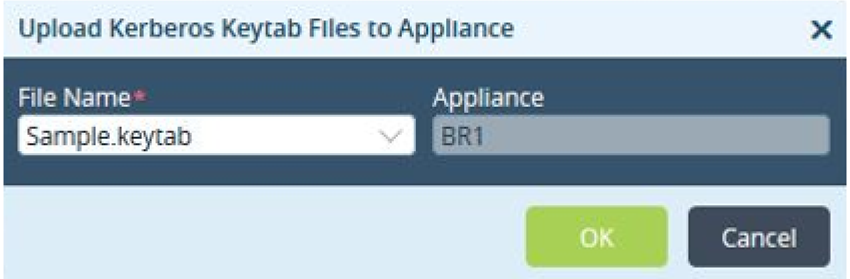
Upload Kerberos Keytab Files to Director ✕

File Name*
Sample.keytab
Browse

Note - Allowed file formats are .keytab

OK Cancel

5. In the Filename field, enter the name of the keytab file, or click the Browse button and then select the file.
6. Click OK to upload the keytab file to the Director node.
7. Select the Appliance tab, and then click the Upload icon to upload the Kerberos keytab file to a VOS device. The Upload Kerberos Keytab Files to Appliance popup window displays.



Upload Kerberos Keytab Files to Appliance ✕

File Name*: Sample.keytab

Appliance: BR1

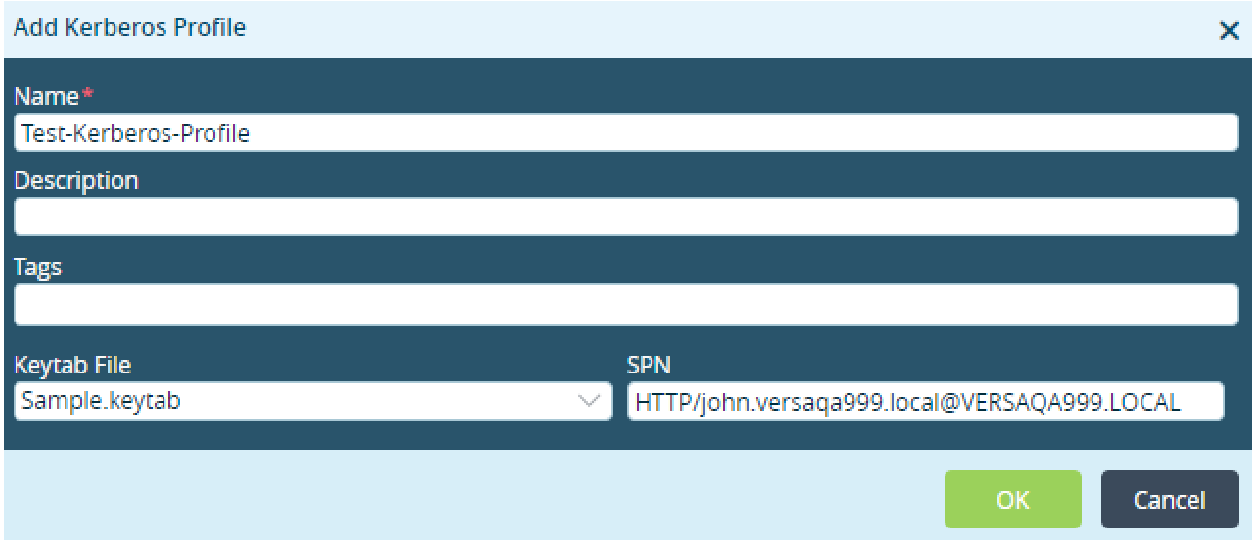
OK Cancel

8. In the Filename field, select the Kerberos keytab file. The Appliance field is populated by default.
9. Click OK.

Configure a Kerberos Profile

To define a Kerberos profile for authenticating a user and group:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Kerberos Profile in the left menu bar
4. Click the Add icon. In Add Kerberos Profile popup window, enter information for the following fields.



Name*: Test-Kerberos-Profile
Description:
Tags:
Keytab File: Sample.keytab
SPN: HTTP/john.versaqa999.local@VERSAQA999.LOCAL

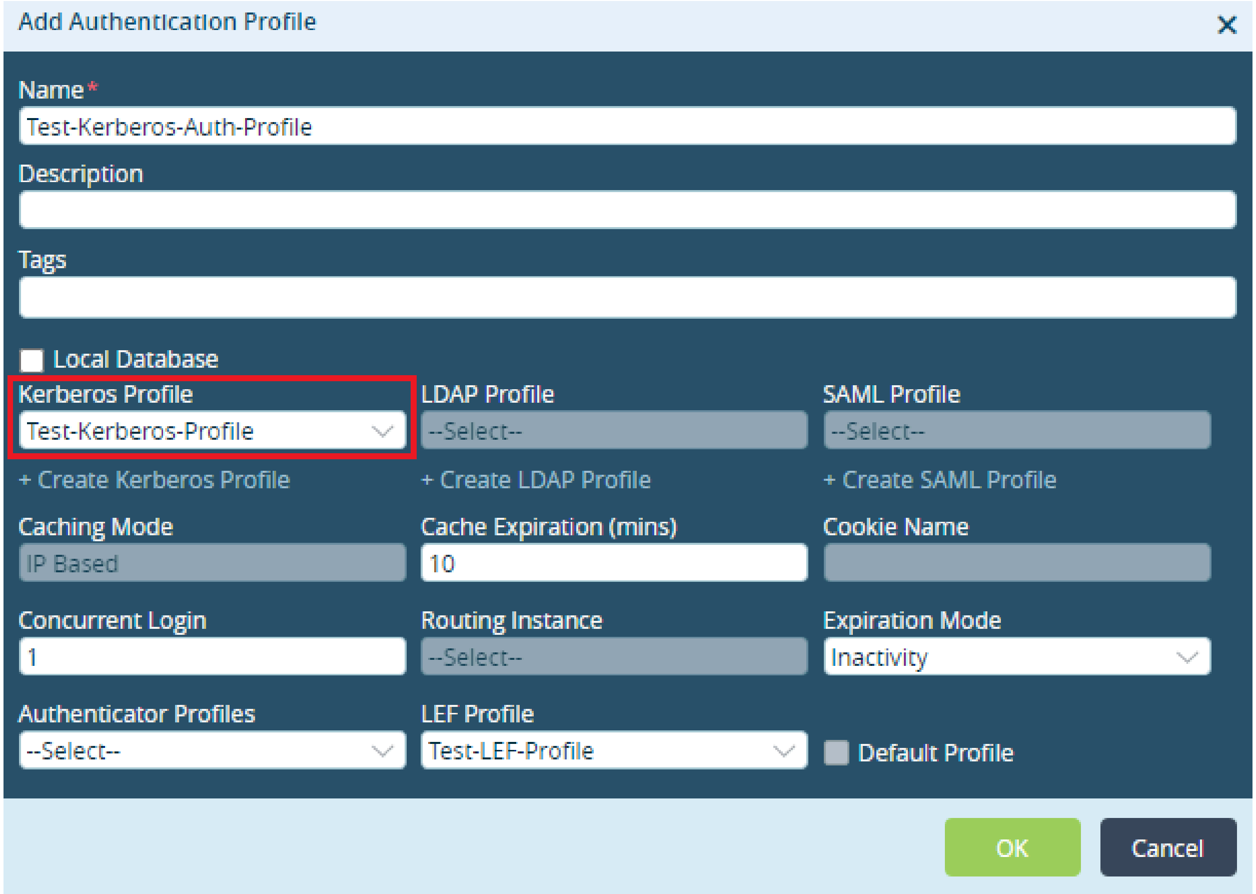
Field	Description
Name	Enter a name for the Kerberos profile.
Description	Enter a text description for the Kerberos profile.
Tags	Enter a keyword or phrase that allows you to filter the Kerberos profile. This is useful when you have many profiles and want to view those that are tagged with a particular keyword.
Keytab File	Select the keytab file that you uploaded in Upload the Kerberos Keytab File, above.
SPN	Enter the value for the service principal name.

5. Click OK.

Configure a Kerberos Authentication Profile and Rule

To define a Kerberos authentication profile that is used in the user and group authentication policy:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Connectors > Users/Groups > Authentication Profiles in the left menu bar.
4. Click the ⊞ Add icon. The Add Authentication Profile popup window displays.
5. In the Kerberos Profile field, select the Kerberos profile you configured in Configure a Kerberos Profile. For information about the other fields in the popup window, see Configure an Authentication Profile.



Add Authentication Profile

Name*
Test-Kerberos-Auth-Profile

Description

Tags

☐ Local Database

Kerberos Profile: Test-Kerberos-Profile
LDAP Profile: --Select--
SAML Profile: --Select--

+ Create Kerberos Profile
+ Create LDAP Profile
+ Create SAML Profile

Caching Mode: IP Based
Cache Expiration (mins): 10
Cookie Name:

Concurrent Login: 1
Routing Instance: --Select--
Expiration Mode: Inactivity

Authenticator Profiles: --Select--
LEF Profile: Test-LEF-Profile
☐ Default Profile

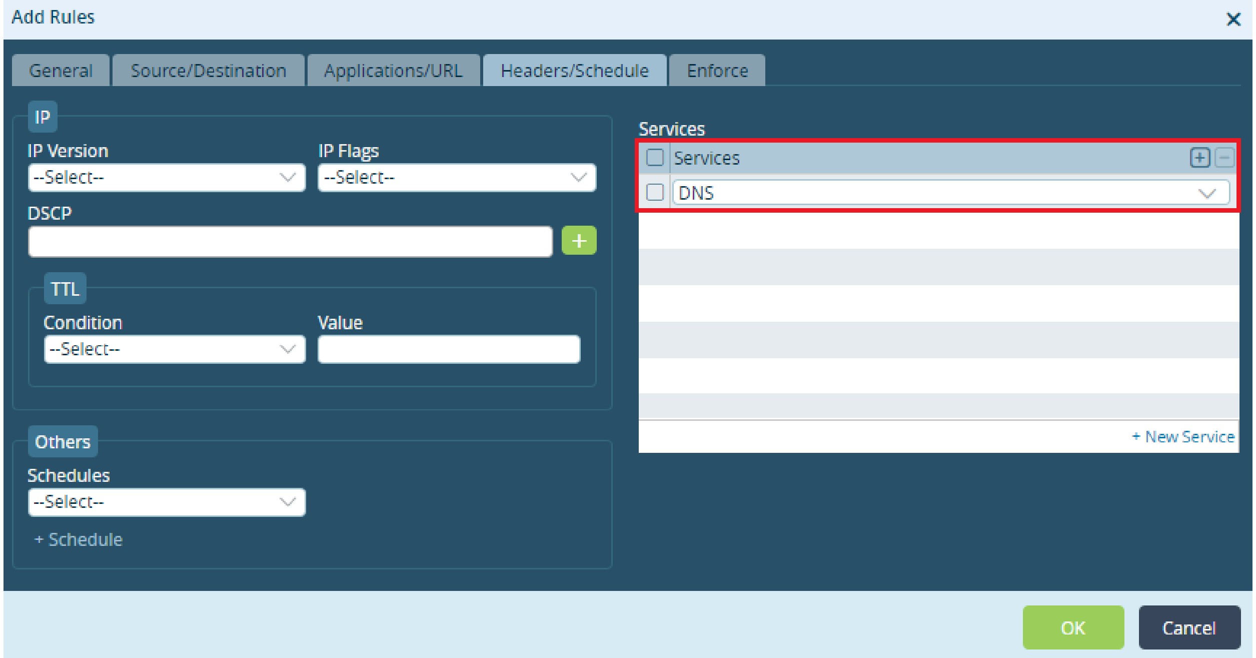
OK
Cancel

6. Click OK.

Configure an Authentication Policy Rule To Bypass DNS Traffic

If you are using DNS server on the internet side, you configure an authentication policy rule to bypass DNS traffic.

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next Gen Firewall > Authentication > Policies in the left menu bar.
4. Select Rules tab and click the Add icon to add a new authentication policy.
5. Select the Header/Schedule tab, and in the Services table, select DNS.



IP Version: --Select--

IP Flags: --Select--

DSCP:

Condition: --Select--

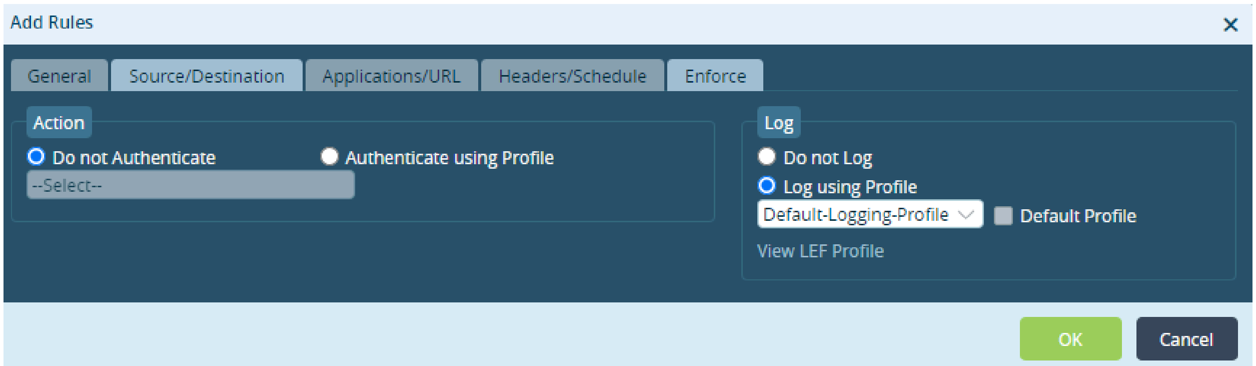
Value:

Schedules: --Select--

Services

□	Services
□	DNS

6. Select the Enforce tab.



● Do not Authenticate ○ Authenticate using Profile

--Select--

○ Do not Log

● Log using Profile

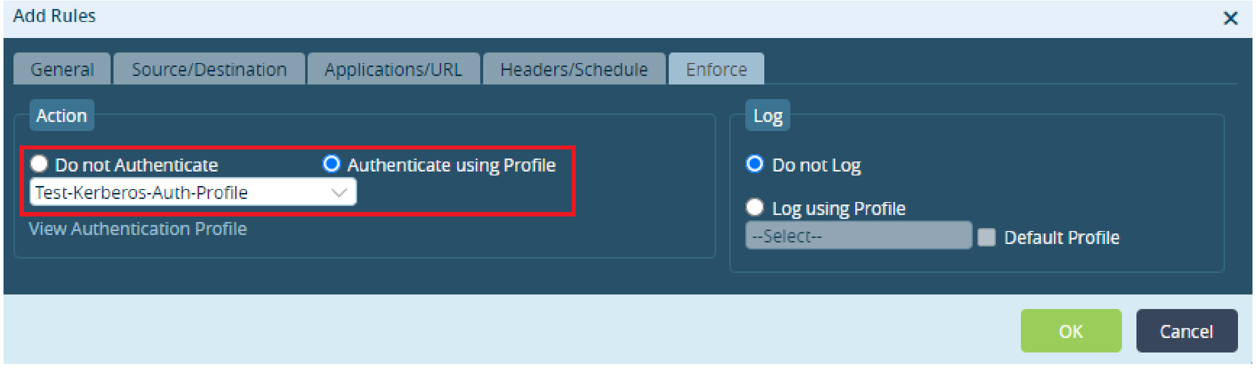
Default-Logging-Profile □ Default Profile

7. Select Do not Authenticate to bypass DNS traffic. Configure other fields in the popup window, as needed. For more information, see Configure Rules for Authentication Policies.
8. Click OK.

Associate an Authentication Profile with an Authentication Policy Rule

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services ⚙ > Next Gen Firewall > Authentication > Policies.

4. Select Rules tab and click the ⊞ Add icon in the dashboard to add a new authentication policy.
5. Select the Enforce tab. In the Action group of fields, select Authenticate Using Profile and then select the Kerberos profile you configured in [Configure a Kerberos Profile](#).



○ Do not Authenticate ● Authenticate using Profile

Test-Kerberos-Auth-Profile

View Authentication Profile

● Do not Log

○ Log using Profile

--Select-- □ Default Profile

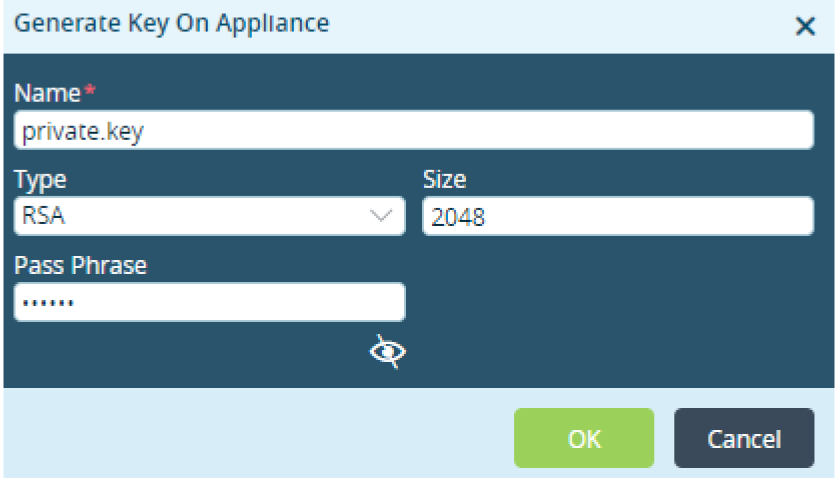
6. Configure other fields in the popup window, as needed. For more information, see [Configure Rules for Authentication Policies](#).
7. Click OK.

Create a Private Key for a CA Certificate

On a VOS device, a key is required to access secured traffic using a certificate. To secure the traffic on a VOS device, you can use either a self-signed CA certificate or a trusted CA certificate.

To create a key for a CA certificate:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > Keys in the left menu bar.
5. Select the Appliance tab and click the Add icon. In the Generate Key on Appliance popup window, enter information for the following fields. For more information, see [Create a CA Certificate Key](#).



Generate Key On Appliance

Name* private.key

Type RSA

Size 2048

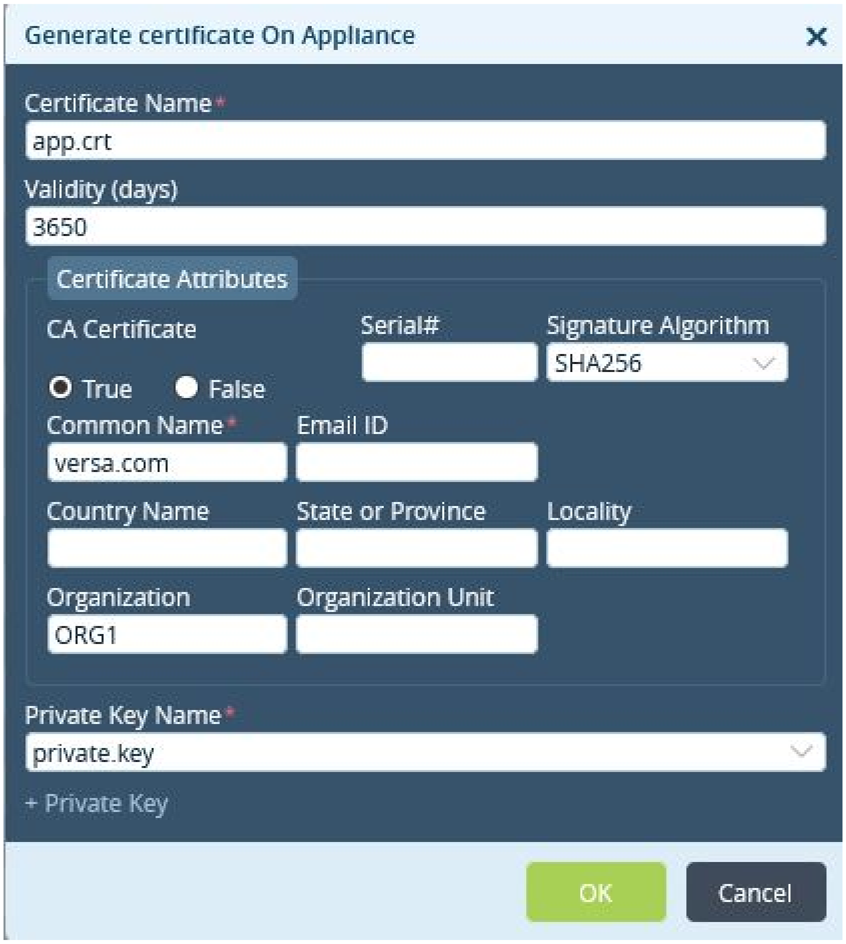
Pass Phrase ••••••

6. Click OK.

Create a CA Certificate

To create a certificate on a VOS device and associate it with a certificate key:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Objects & Connectors > Objects > Custom Objects > Certificates in the left menu bar.
5. Select the Appliance tab and click the Add icon. In the Generate Certificate on Appliance popup window, enter information for the following fields. For more information, see Create a Certificate on a VOS Device.



Certificate Name*: app.crt

Validity (days): 3650

CA Certificate: ● True ○ False

Serial#:

Signature Algorithm: SHA256

Common Name*: versa.com

Email ID:

Country Name:

State or Province:

Locality:

Organization: ORG1

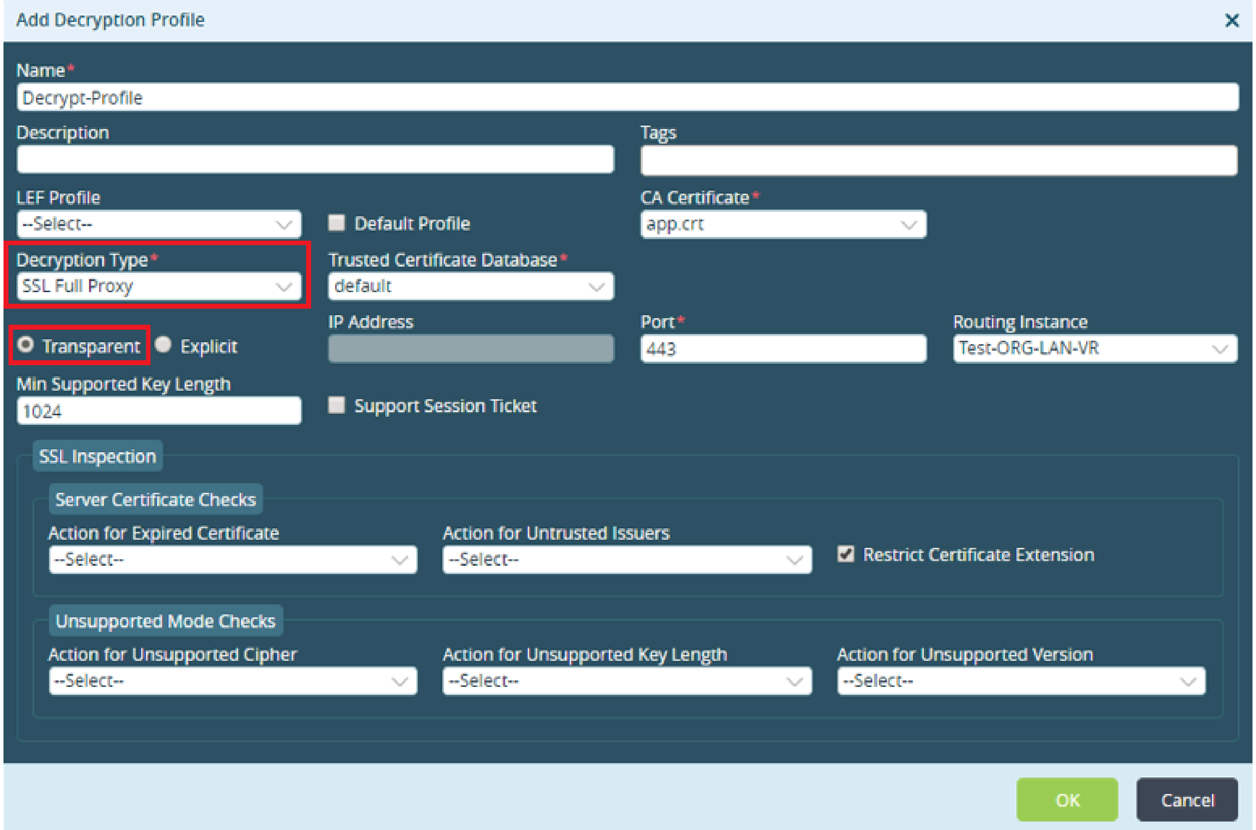
Organization Unit:

Private Key Name*: private.key

6. Click OK.

Configure Transparent Proxy for Kerberos

1. Configure a decryption profile in transparent mode:
    a. In Appliance view, select the Configuration tab in the top menu bar.
    b. Select an organization in the horizontal menu bar.
    c. Select Services > Next Gen Firewall > Decryption > Profiles in the left menu bar.
    d. Click the ⊞ Add icon. The Add Decryption Profile popup window displays. For more information, see Configure an SSL Decryption Profile.



Add Decryption Profile

Name* Decrypt-Profile

Description

Tags

LEF Profile --Select--

□ Default Profile

CA Certificate* app.crt

Decryption Type* SSL Full Proxy

Trusted Certificate Database* default

● Transparent ○ Explicit

IP Address

Port* 443

Routing Instance Test-ORG-LAN-VR

Min Supported Key Length 1024

□ Support Session Ticket

SSL Inspection

Server Certificate Checks

Action for Expired Certificate --Select--

Action for Untrusted Issuers --Select--

☑ Restrict Certificate Extension

Unsupported Mode Checks

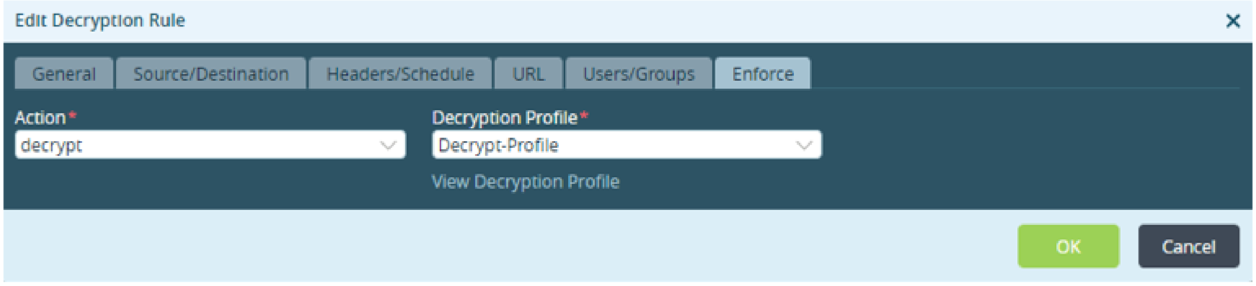
Action for Unsupported Cipher --Select--

Action for Unsupported Key Length --Select--

Action for Unsupported Version --Select--

   e. In the Decryption Type field, select SSL Full Proxy.
   f. Select Transparent.
   g. Click OK.

2. Associate the transparent decryption profile with a decryption policy rule:
   a. Select Services > Next Gen Firewall > Decryption > Policies in the left menu bar.
   b. Select the Rules tab and click the ⊞ Add icon. The Add Decryption Rule popup window displays.
   c. Select the Enforce tab. In the Action field, select decrypt, and in the Decryption Profile field select the decryption profile you configured in Step 1. For more information, see Configure an SSL Decryption Policy Rule.



Edit Decryption Rule

Action* decrypt

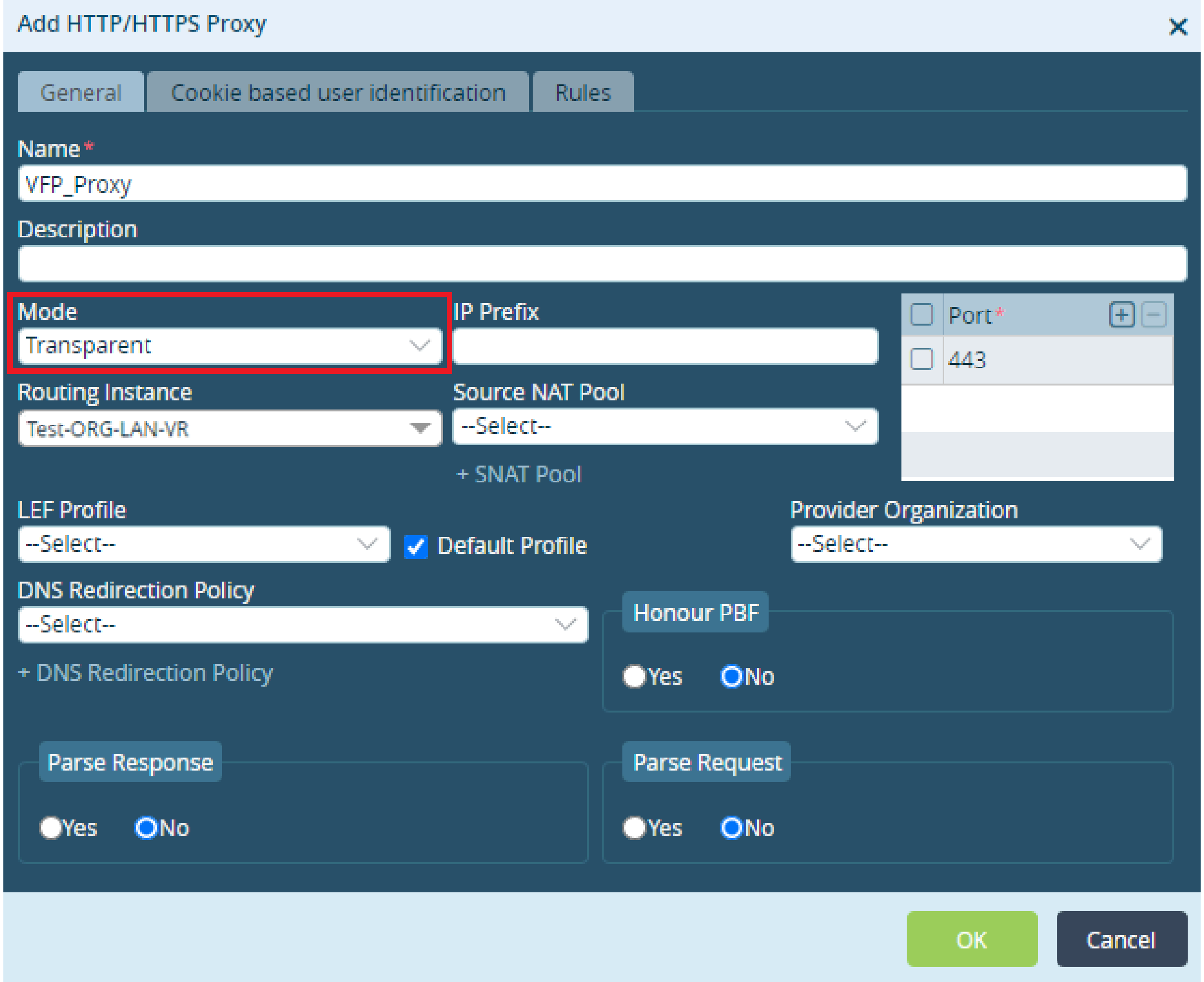
Decryption Profile* Decrypt-Profile

   d. Click OK.

3. Configure a transparent secure web proxy:

a. In Appliance view, select the Configuration tab in the top menu bar.
b. Select an organization in the horizontal menu bar.

c. Select Services > Web Proxy in the left menu bar. The Add HTTP/HTTPS Proxy window displays.
d. Select Transparent from the Mode drop-down list and enter other details. For more information, see Configure a Transparent Proxy.
e. Enter the port number.



Add HTTP/HTTPS Proxy

Name* VFP_Proxy

Description

Mode: Transparent

IP Prefix

Port*: 443

Routing Instance: Test-ORG-LAN-VR

Source NAT Pool: --Select--

LEF Profile: --Select--

☑ Default Profile

Provider Organization: --Select--

DNS Redirection Policy: --Select--

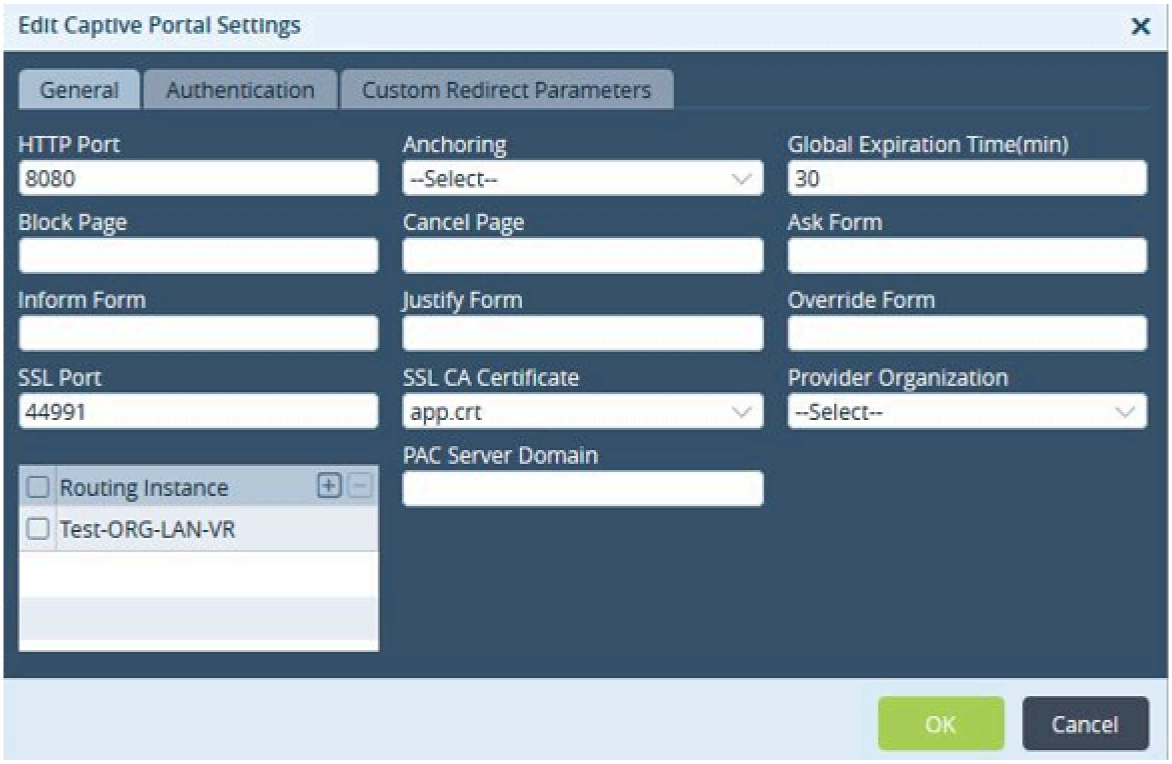
Honour PBF: ○ Yes ● No

Parse Response: ○ Yes ● No

Parse Request: ○ Yes ● No

f. Click OK.

4. Configure a transparent captive portal:
   a. In Appliance view, select the Configuration tab in the top menu bar.
   b. Select Services > Next Gen Firewall > Security Settings > Captive Portal in the left menu bar. The dashboard displays the Captive Portal Settings pane.
   c. Click the Edit icon. The Edit Captive Portal Settings popup window displays. For more information, see Modify Captive Portal Settings.
   d. Select the General tab, and enter information for the following fields:

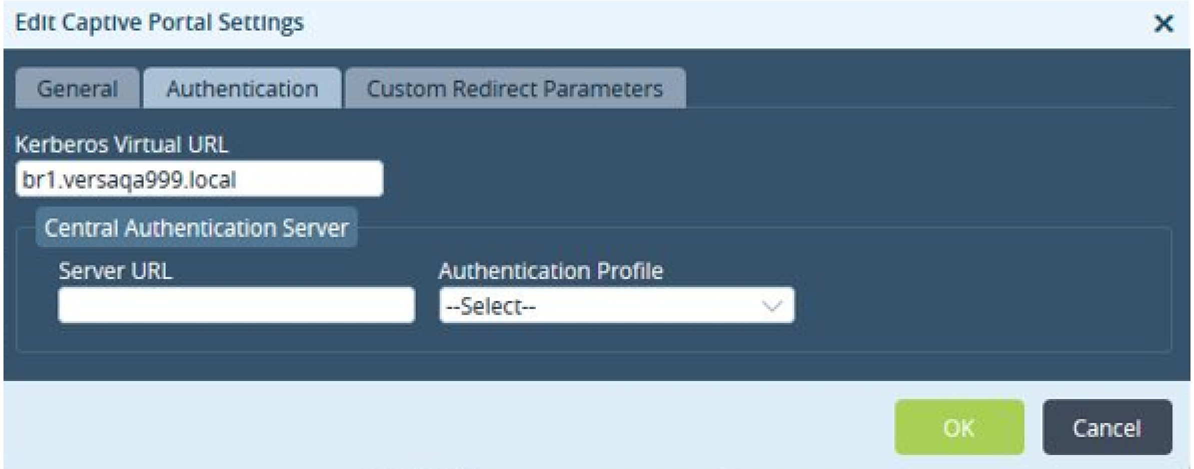


HTTP Port: 8080
Anchoring: --Select--
Global Expiration Time(min): 30
Block Page:
Cancel Page:
Ask Form:
Inform Form:
Justify Form:
Override Form:
SSL Port: 44991
SSL CA Certificate: app.crt
Provider Organization: --Select--
PAC Server Domain:

□ Routing Instance
□ Test-ORG-LAN-VR

i. In the SSL CA Certificate field, select the CA certificate.
ii. In the SSL Port field, enter the SSL port number (here, port 44991).
iii. In the Routing Instance table, select the routing instance.

e. Select the Authentication tab, and in the Kerberos Virtual URL field, enter the Kerberos virtual URL. Note that you must resolve the virtual URL with the appliance LAN IP address.


Edit Captive Portal Settings
General
Authentication
Custom Redirect Parameters
Central Authentication Server
OK
Cancel

Kerberos Virtual URL: br1.versaqa999.local
Server URL:
Authentication Profile: --Select--

f. Click OK.

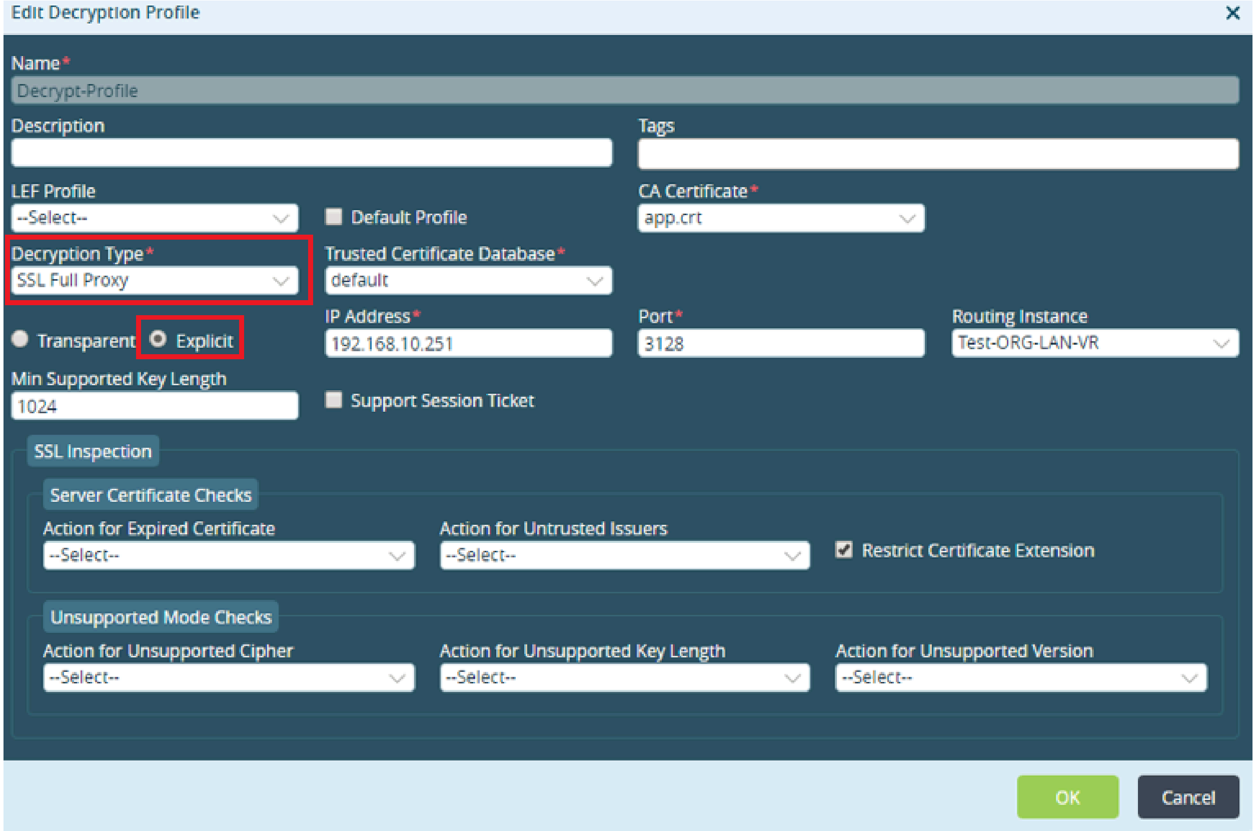
Configure Kerberos Setting in Client Browser for Transparent Proxy

A transparent proxy processes SSL/TLS traffic that is destined to any IP address but to a particular port. The client (browser) performs DNS resolution and opens the connection to the server's IP address. For more information, see Enable Kerberos Settings in Browsers below.

Configure an Explicit Proxy for Kerberos

An explicit proxy processes SSL/TLS traffic destined to a specific IP address and a port.

1. Configure a decryption profile in explicit mode:
   a. In Appliance view, select the Configuration tab in the top menu bar.
   b. Select an organization in the horizontal menu bar.
   c. Select Services > Next Gen Firewall > Decryption > Profiles in the left menu bar.
   d. Click the Add icon. The Add Decryption Profile popup window displays. For more information, see Configure an SSL Decryption Profile.



Edit Decryption Profile

Name* Decrypt-Profile

Description

Tags

LEF Profile --Select--

□ Default Profile

CA Certificate* app.crt

Decryption Type* SSL Full Proxy

Trusted Certificate Database* default

○ Transparent ● Explicit

IP Address* 192.168.10.251

Port* 3128

Routing Instance Test-ORG-LAN-VR

Min Supported Key Length 1024

□ Support Session Ticket

SSL Inspection

Server Certificate Checks

Action for Expired Certificate --Select--

Action for Untrusted Issuers --Select--

☑ Restrict Certificate Extension

Unsupported Mode Checks

Action for Unsupported Cipher --Select--

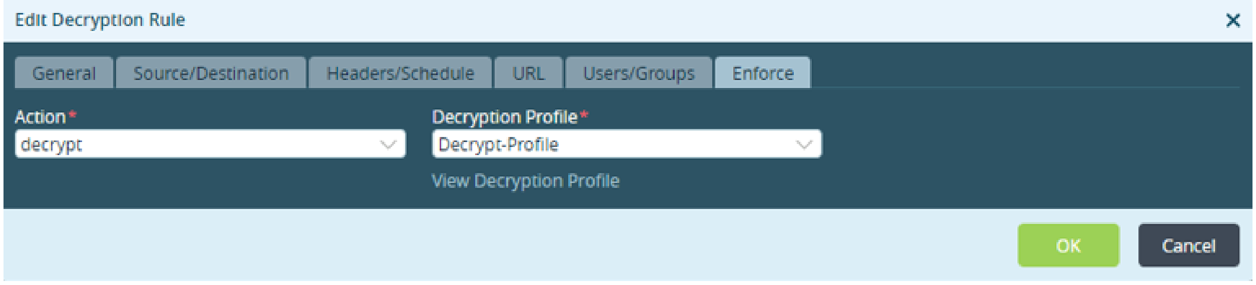
Action for Unsupported Key Length --Select--

Action for Unsupported Version --Select--

   e. In the Decryption Type field, select SSL Full Proxy.
   f. Select Explicit.
   g. Enter IP address and port number of the proxy, and select the routing instance to use to reach the proxy.

h. Click OK.

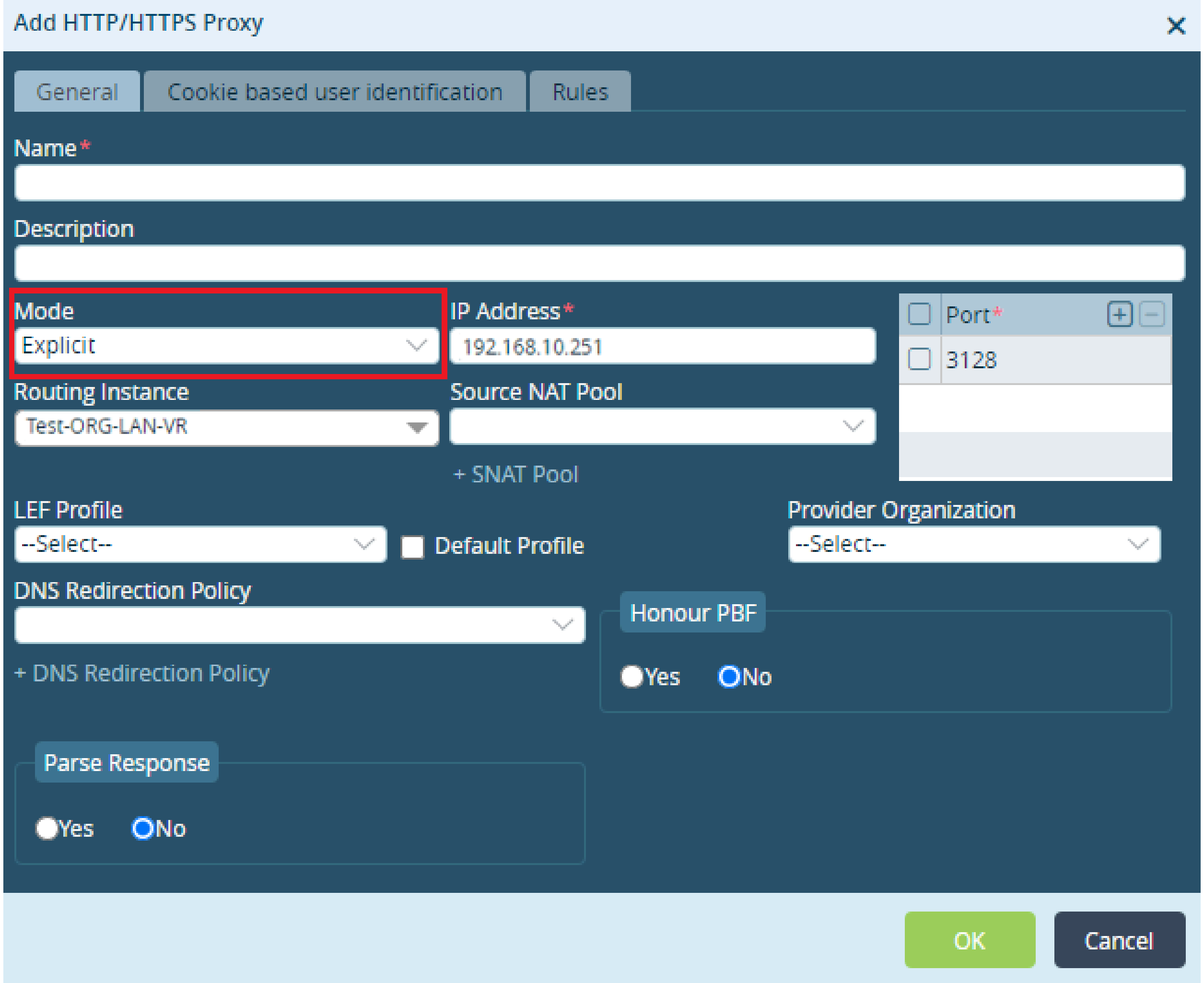
2. Associate the explicit decryption profile with a decryption policy rule:
   a. Select Services > Next Gen Firewall > Decryption > Policies in the left menu bar.
   b. Select the Rules tab and click the Add ico. The Add Decryption Rule popup window displays.
   c. Select the Enforce tab. In the Action field, select Decrypt, and in the Decryption Profile field, select the decryption profile you configured in Step 1. For more information, see Configure an SSL Decryption Policy Rule.



Action* decrypt

Decryption Profile* Decrypt-Profile

3. Configure an explicit secure web proxy:
   a. Select the Configuration tab in the top menu bar.
   b. Select an organization in the horizontal menu bar.
   c. Select Services > Web Proxy in the left menu bar. The Add HTTP/HTTPS Proxy window displays.
   d. In the Mode field, select Explicit, and enter information for other fields. For more information, see Configure an Explicit Proxy.



Name*

Description

Mode: Explicit

IP Address*: 192.168.10.251

□ Port*
□ 3128

Routing Instance: Test-ORG-LAN-VR

Source NAT Pool

LEF Profile: --Select--

□ Default Profile

Provider Organization: --Select--

DNS Redirection Policy

Honour PBF: ○ Yes ● No

Parse Response: ○ Yes ● No

e. Click OK.

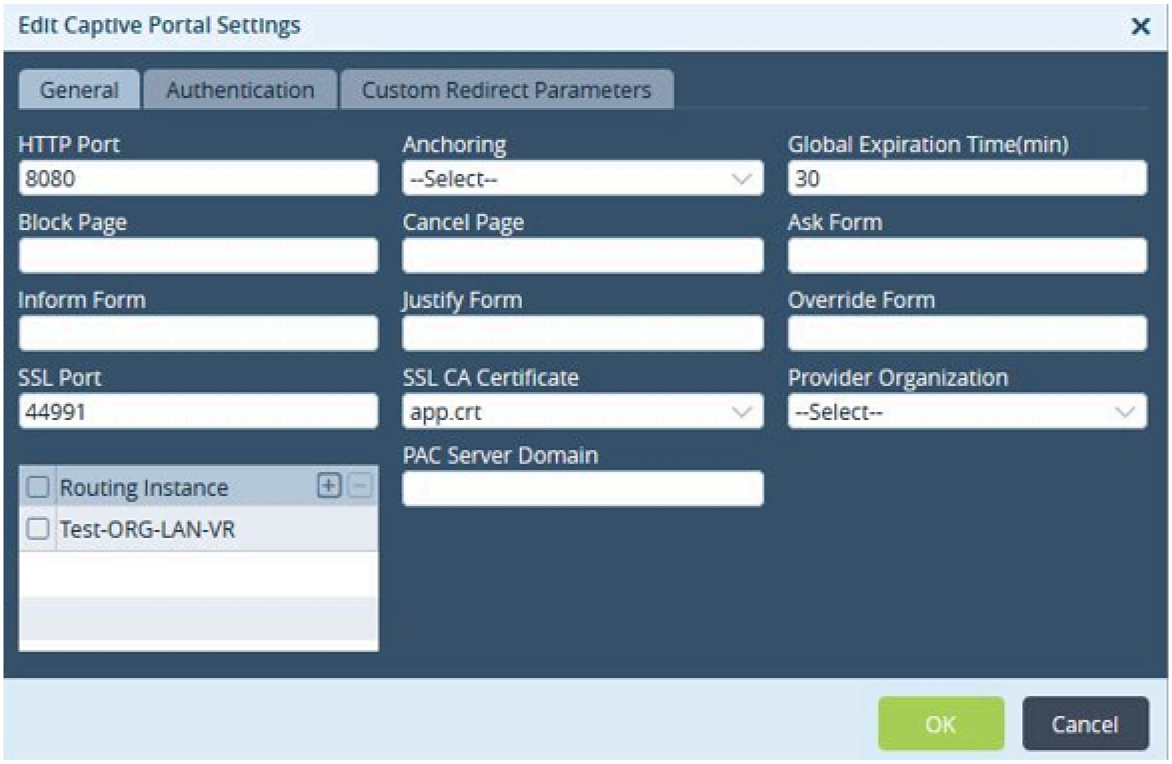
4. Configure an explicit captive portal:

   a. In Appliance view, select the Configuration tab in the top menu bar.

   b. Select Services > Next Gen Firewall > Security Settings > Captive Portal in the left menu bar. The dashboard displays the Captive Portal Settings pane.

   c. Click the Edit icon. The Edit Captive Portal Settings popup window displays. For more information, see Modify Captive Portal Settings.

   d. Select the General tab, and enter information for the following fields:



Edit Captive Portal Settings

HTTP Port: 8080

Anchoring: --Select--

Global Expiration Time(min): 30

Block Page:

Cancel Page:

Ask Form:

Inform Form:

Justify Form:

Override Form:

SSL Port: 44991

SSL CA Certificate: app.crt

Provider Organization: --Select--

PAC Server Domain:

□ Routing Instance
□ Test-ORG-LAN-VR

i. In the SSL CA Certification field, select the CA certificate.

ii. In the SSL Port field, enter the port number for the captive portal.

iii. In the Routing Instance table, select the routing instance to use to reach the captive portal.

e. Click OK.

Configure Kerberos Setting in Client Browser for Explicit Proxy

An explicit proxy processes SSL/TLS traffic destined to a specific IP address and a specific port. On the browser client, you configure the proxy IP address and the port. For more information, see Enable Kerberos Settings in Browsers below.

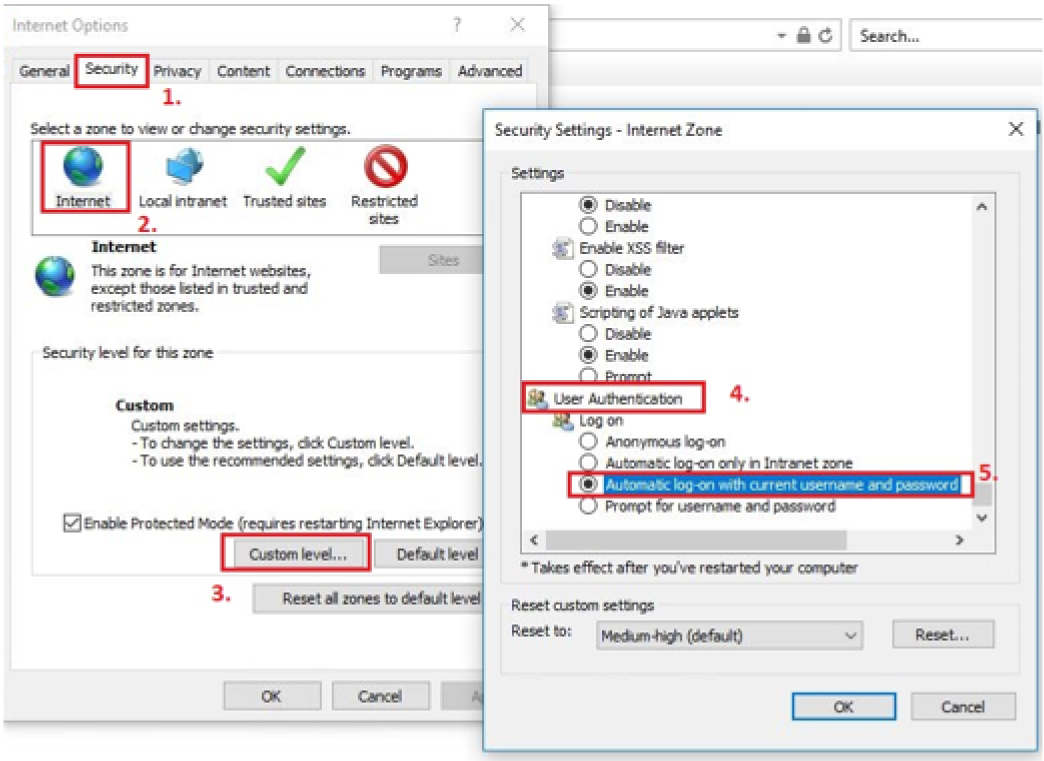
Enable Kerberos Settings in Browsers

As part of the configuring Kerberos authentication, you must enable Kerberos settings in browsers for transparent and explicit web proxy. This article describes the settings to enable Kerberos for Internet Explorer (IE) and Mozilla Firefox. The settings for IE are applicable for Google Chrome as well.

Enable Kerberos in Internet Explorer for Transparent Proxy

1. Open an IE browser window.
2. Click the Settings icon in the upper-right corner, or click the Tools menu.

3. Select Internet Options, and select the Security tab.
4. Select Internet, and click Custom Level. The Security Setting dialog box displays.
5. In User Authentication > Log On, click Automatic Log-On with Current Username and Password.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

Settings

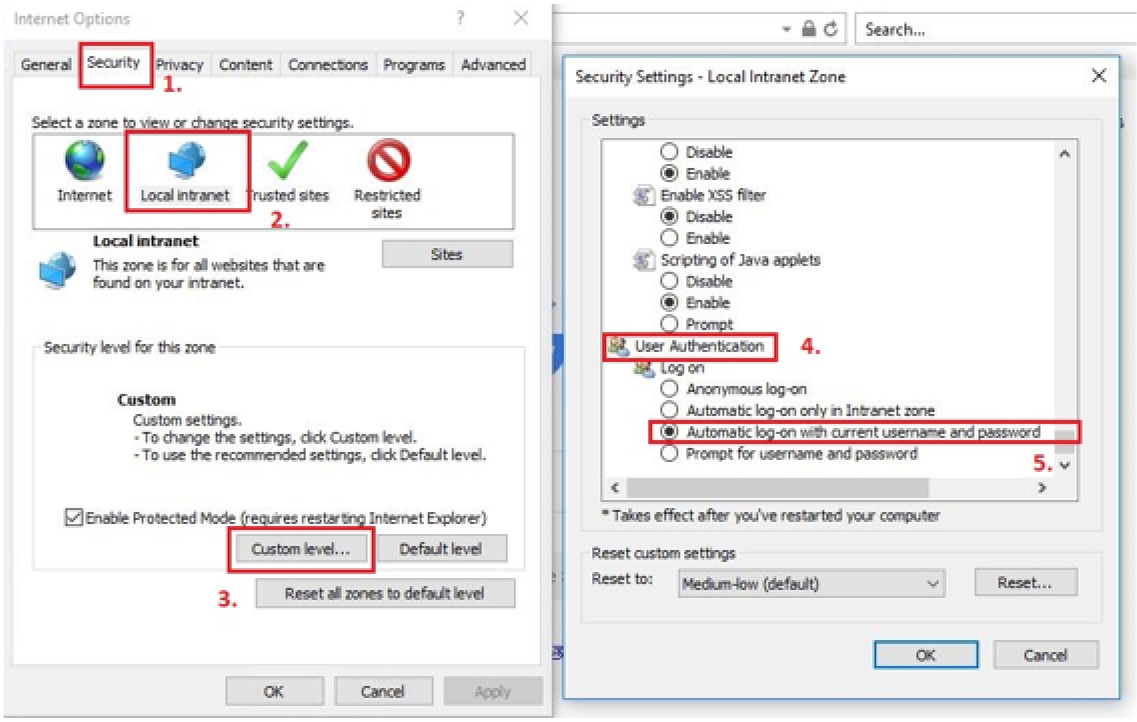
● Disable
○ Enable
Enable XSS filter
○ Disable
● Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Log on
○ Anonymous log-on
○ Automatic log-on only in Intranet zone
● Automatic log-on with current username and password
○ Prompt for username and password

*Takes effect after you've restarted your computer

Reset custom settings

Reset to: Medium-high (default)

6. Select Security tab again, and select Local Intranet and repeat Steps 4 and 5.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

1.

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

2.

Local intranet

This zone is for all websites that are found on your intranet.

Sites

Security level for this zone

Custom

Custom settings.

- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

3.

Reset all zones to default level

OK | Cancel | Apply

Security Settings - Local Intranet Zone

Settings

○ Disable
● Enable

Enable XSS filter

● Disable
○ Enable

Scripting of Java applets

○ Disable
● Enable
○ Prompt

User Authentication 4.

Log on

○ Anonymous log-on
○ Automatic log-on only in Intranet zone
● Automatic log-on with current username and password
○ Prompt for username and password 5.

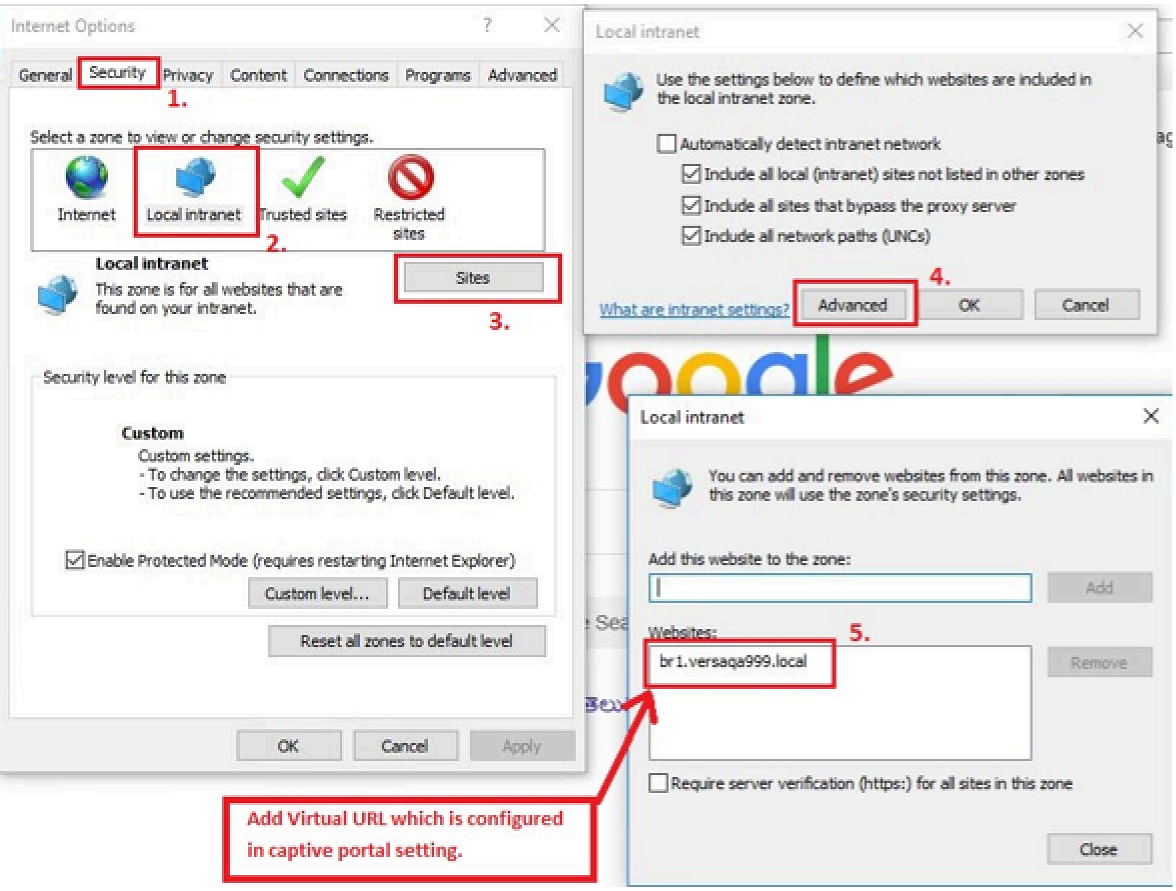
*Takes effect after you've restarted your computer

Reset custom settings

Reset to: Medium-low (default) | Reset...

OK | Cancel

7. Under Local Intranet, select Sites. The Local Intranet dialog box displays.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

1.

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

2.

Local intranet

This zone is for all websites that are found on your intranet.

Sites 3.

Security level for this zone

Custom

Custom settings.

- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☐ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

☑ Include all sites that bypass the proxy server

☑ Include all network paths (UNCs)

What are intranet settings? | Advanced 4. | OK | Cancel

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

Websites: 5.

br1.versaqa999.local

Remove

☐ Require server verification (https:) for all sites in this zone

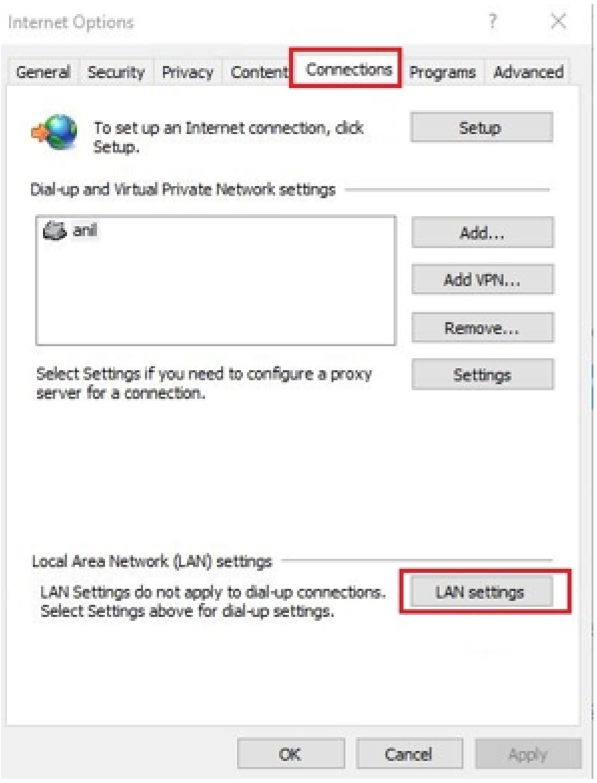
Close

Add Virtual URL which is configured in captive portal setting.

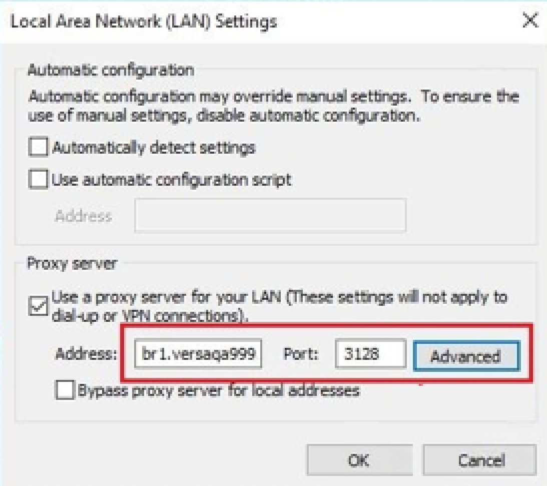
8. Click Advanced, and in the Websites field, enter the virtual URL that you configured in Step 3 of Configure Transparent Proxy for Kerberos above.
9. Click Close.
10. Click OK.

Enable Kerberos in Internet Explorer for Explicit Proxy

1. Perform Steps 1 through 10 in Enable Kerberos in Internet Explorer for Transparent Proxy above.
2. In Internet Options, select the Connections tab.


Internet Options
?
General
Security
Privacy
Content
Connections
Programs
Advanced
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
anil
Add...
Add VPN...
Remove...
Select Settings if you need to configure a proxy server for a connection.
Settings
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Select Settings above for dial-up settings.
LAN settings
OK
Cancel
Apply

3. Click LAN Settings. The Local Area Network (LAN) Settings dialog box displays.
4. Click Use a Proxy Server for Your LAN.
5. In the Address field, enter the virtual URL that you configured in Step 3 of Configure Transparent Proxy for Kerberos above.
6. In the Port field, enter the proxy port number.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

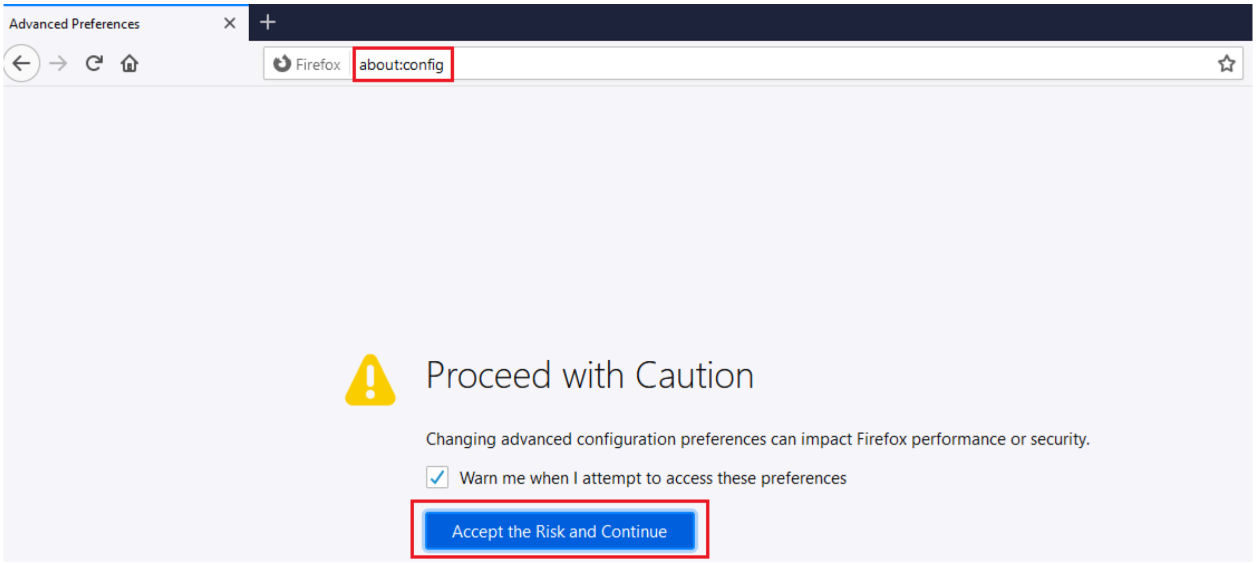
Address: br1.versaqa999 Port: 3128

□ Bypass proxy server for local addresses

7. Click OK.

Enable Kerberos in Firefox for Transparent Proxy

1. Open a Firefox browser window, type about:config in the address bar, and press Enter.



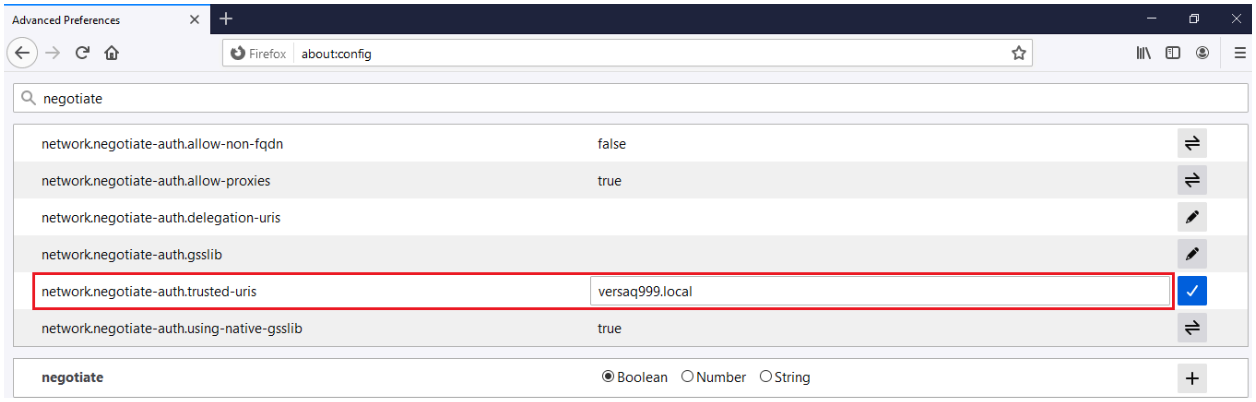
about:config

Proceed with Caution

Changing advanced configuration preferences can impact Firefox performance or security.

☑ Warn me when I attempt to access these preferences

2. Click Accept the Risk and Continue.
3. In the search bar, enter the string "negotiate", and press Enter.



negotiate

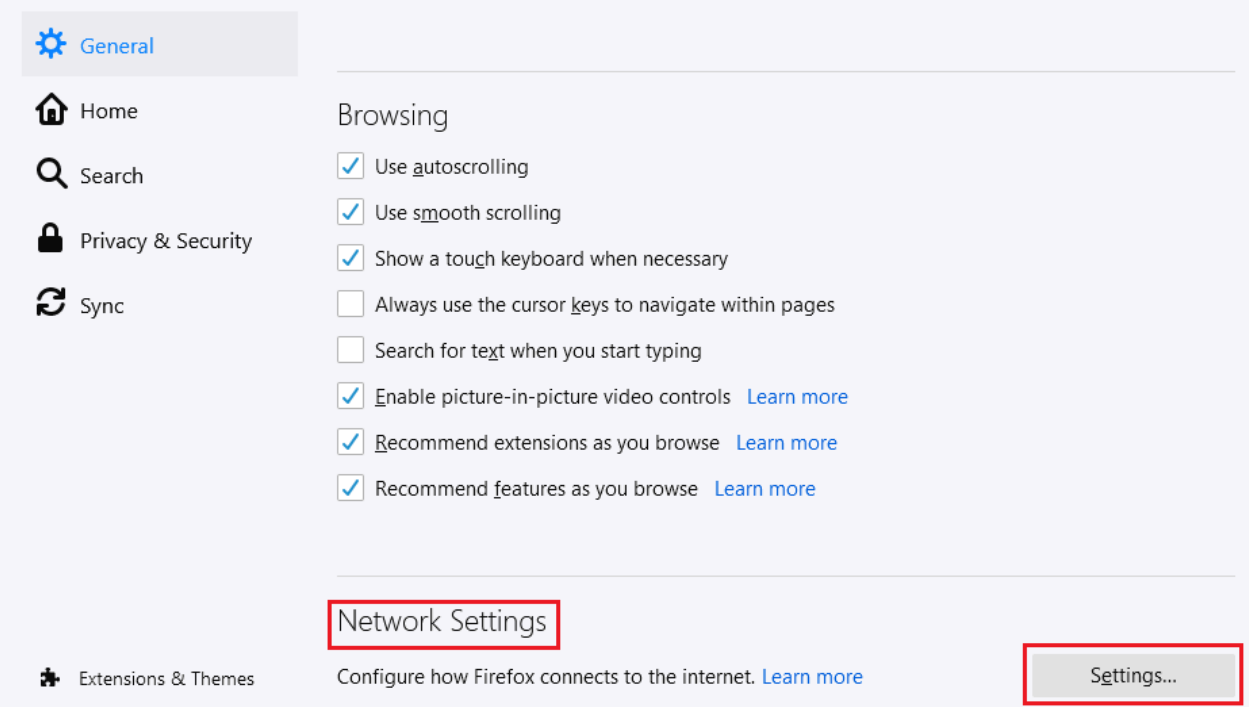
network.negotiate-auth.allow-non-fqdn	false
network.negotiate-auth.allow-proxies	true
network.negotiate-auth.delegation-uris	
network.negotiate-auth.gsslib	
network.negotiate-auth.trusted-uris	versaq999.local
network.negotiate-auth.using-native-gsslib	true

negotiate ● Boolean ○ Number ○ String

4. Select network.negotiate-auth.trusted-uris, and enter the domain name.

Enable Kerberos in Firefox for Explicit Proxy

1. Perform Steps 1 through 4 in Enable Kerberos in Firefox for Transparent Proxy above.
2. In the main menu, select Options.
3. Navigate to General > Network Setting and click Settings. The Connection Settings dialog box displays.



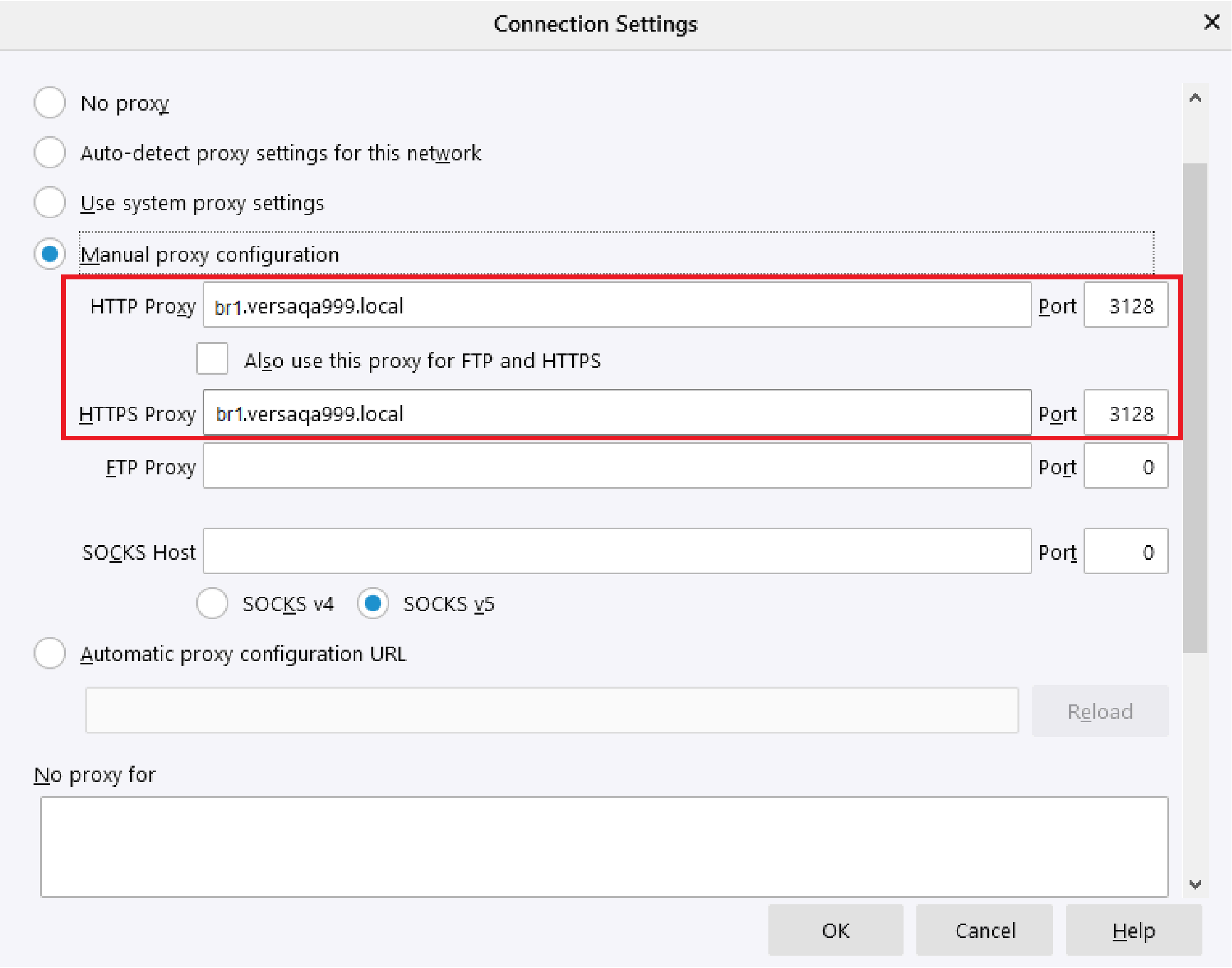
Browsing

☑ Use autoscrolling
☑ Use smooth scrolling
☑ Show a touch keyboard when necessary
☐ Always use the cursor keys to navigate within pages
☐ Search for text when you start typing
☑ Enable picture-in-picture video controls Learn more
☑ Recommend extensions as you browse Learn more
☑ Recommend features as you browse Learn more

Network Settings

Configure how Firefox connects to the internet. Learn more

4. In Configure Proxy Access to the Internet, select Manual Proxy Configurationn.



Connection Settings

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy br1.versaqa999.local Port 3128

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy br1.versaqa999.local Port 3128

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

5. In the HTTP and HTTPS Proxy fields, enter the virtual URL that you configured in Step 3 of Configure Transparent Proxy for Kerberos above.
6. Click OK.

Match Authenticated Users

To configure match criteria for the specific user authenticated by Kerberos in a CoS (QoS), NGFW, SD-WAN, or UTM policy rule, see Add External Database Users in Configure User and Group Policy.

View Active Users

To view currently active users:

1. Import the SSL CA certificate to the browser.
2. Log in using the domain user name in the domain client system and browse the internet. User login is automatic in a device with the domain username.

3. Verify the list of active users by issuing the **show orgs org-services** *organization-name* **user-identification live-users list detail** CLI command.
   For example:

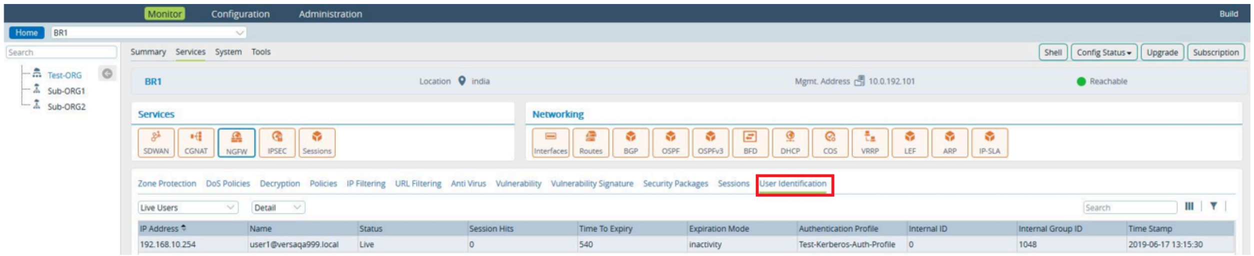
```
admin@BR1-cli> show orgs org-services ORG1 user-identification live-users list detail
                                                     TIME
                                             SESSION  TO     EXPIRATION  SEQUENCE
INFORMATION                                 INTERNAL
IP ADDRESS      NAME                    STATUS  HITS     EXPIRY  MODE       NUMBER    SOURCE
AUTHENTICATION PROFILE      ID       INTERNAL GROUP ID       TIME STAMP
--------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------
192.168.10.254  user1@versaqa999.local  Live    72      119    inactivity  -       n/a        Test-Kerberos-
Auth-Profile  -          [ 1048 ]             2020-11-06 11:16:24
```

Monitor Kerberos User Identification Statistics

To view the reports for Kerberos authentication profiles (in this case, Kerberos authentication profile) associated with a user ID, you monitor user identification statistics. For more information, see Monitor Device Services.

To monitor active user statistics:

1. Select the Administration tab in the top menu bar.
   a. Select Appliances in the left menu bar.
   b. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Provider Organization > Services tab.
4. Select NGFW NGFW > User Identification, and select Live Users from the drop-down list. The user ID statistics displays.



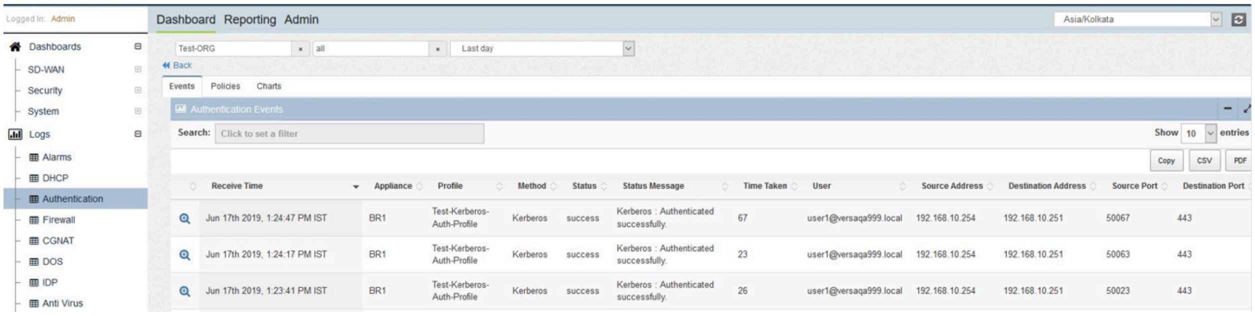
Live Users
Detail

IP Address	Name	Status	Session Hits	Time To Expiry	Expiration Mode	Authentication Profile	Internal ID	Internal Group ID	Time Stamp
192.168.10.254	user1@versaqa999.local	Live	0	540	inactivity	Test-Kerberos-Auth-Profile	0	1048	2019-06-17 13:15:30

Display Kerberos Authentication Logs

To display the authentication events logs for a Kerberos authentication profile:

3. In Director view, select the Analytics tab from the top menu bar. The view changes to Analytics view.
4. Select Home > Logs > Authentication in the left menu bar to view the authentication logs.
5. Select the Events tab to display information about the authentication logs.



Receive Time	Appliance	Profile	Method	Status	Status Message	Time Taken	User	Source Address	Destination Address	Source Port	Destination Port
Jun 17th 2019, 1:24:47 PM IST	BR1	Test-Kerberos-Auth-Profile	Kerberos	success	Kerberos : Authenticated successfully.	67	user1@versaqa999.local	192.168.10.254	192.168.10.251	50067	443
Jun 17th 2019, 1:24:17 PM IST	BR1	Test-Kerberos-Auth-Profile	Kerberos	success	Kerberos : Authenticated successfully.	23	user1@versaqa999.local	192.168.10.254	192.168.10.251	50063	443
Jun 17th 2019, 1:23:41 PM IST	BR1	Test-Kerberos-Auth-Profile	Kerberos	success	Kerberos : Authenticated successfully.	26	user1@versaqa999.local	192.168.10.254	192.168.10.251	50023	443

Supported Software Information

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

Additional Information

Configure HTTP/HTTPS Proxy
Configure LDAP for End-User Authentication
Configure URL Filtering
Configure User and Group Policy
Monitor Device Services