Citrix NetScaler Two-Factor Authentication (2FA)

logintc.com/docs/connectors/citrix-netscaler

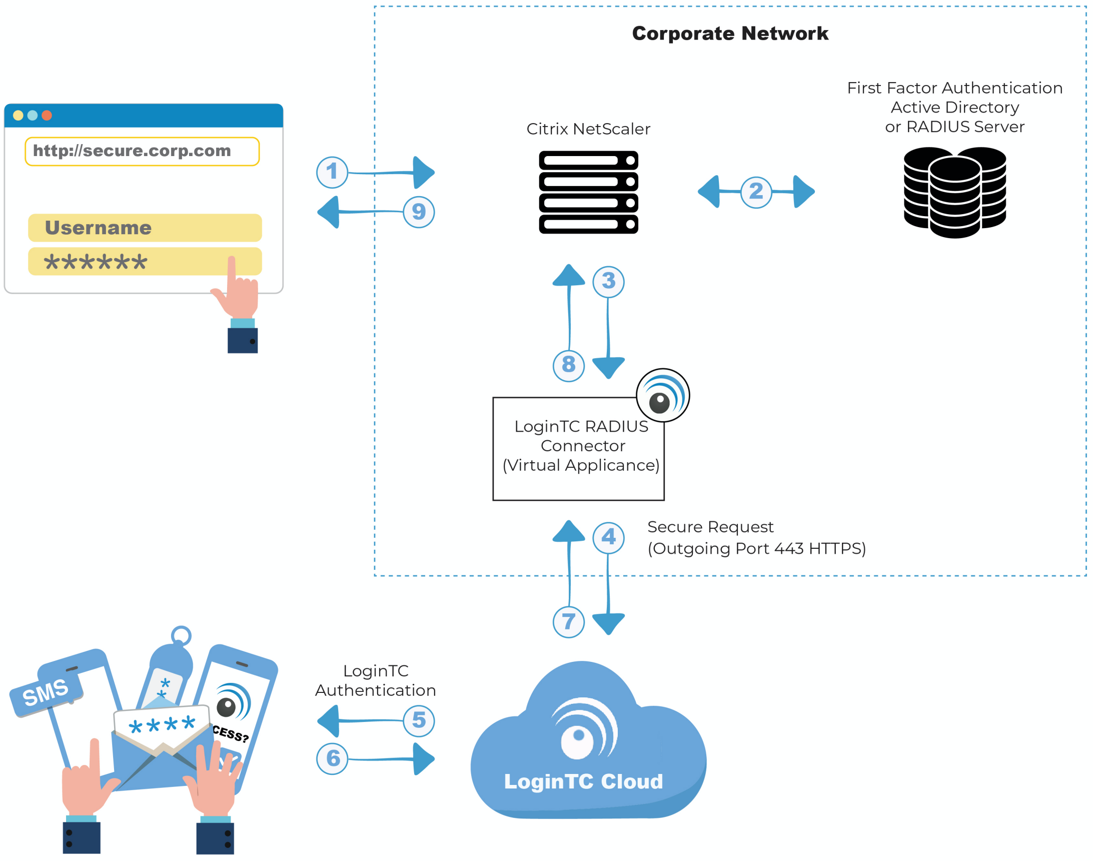
The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables Citrix NetScaler to use LoginTC for the most secure two-factor authentication.

Subscription Requirement
Your organization requires the **Business** or **Enterprise** plan to use the Iframe mode of the LoginTC RADIUS Connector. See the Pricing page for more information about subscription options.

User Experience
There are a wide variety of authentication mechanism users can use to perform MFA with Citrix Gateway/ADC/NetScaler product suite.

Watch Video At: https://youtu.be/iRDcJosDLP8

Architecture



Authentication Flow

1. A user attempts access with username / password
2. The username / password is verified against an existing first factor directory (LDAP, Active Directory or RADIUS)
3. A RADIUS authentication request is sent to the LoginTC RADIUS Connector
4. An authentication request is made to LoginTC Cloud Services
5. Secure push notification request sent to the user’s mobile or desktop device
6. User response (approval or denial of request) sent to LoginTC Cloud Services
7. The LoginTC RADIUS Connector polls until the user responds or a timeout is reached
8. RADIUS Access-Accept sent back to Citrix NetScaler
9. User is granted access to Citrix NetScaler

Compatibility

Citrix NetScaler compatibility:

Citrix NetScaler 10.0+ (Including MPX, VPX and SDX appliances)

Appliance not listed?
We probably support it. Contact us if you have any questions.

Prerequisites
Before proceeding, please ensure you have the following:

- LoginTC Admin Panel account
- Computer virtualization software such as VMware ESXi, VirtualBox, or Hyper-V
- Virtual Machine requirements:
  - 2048 MB RAM
  - 8 GB disk size

Create Application
Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

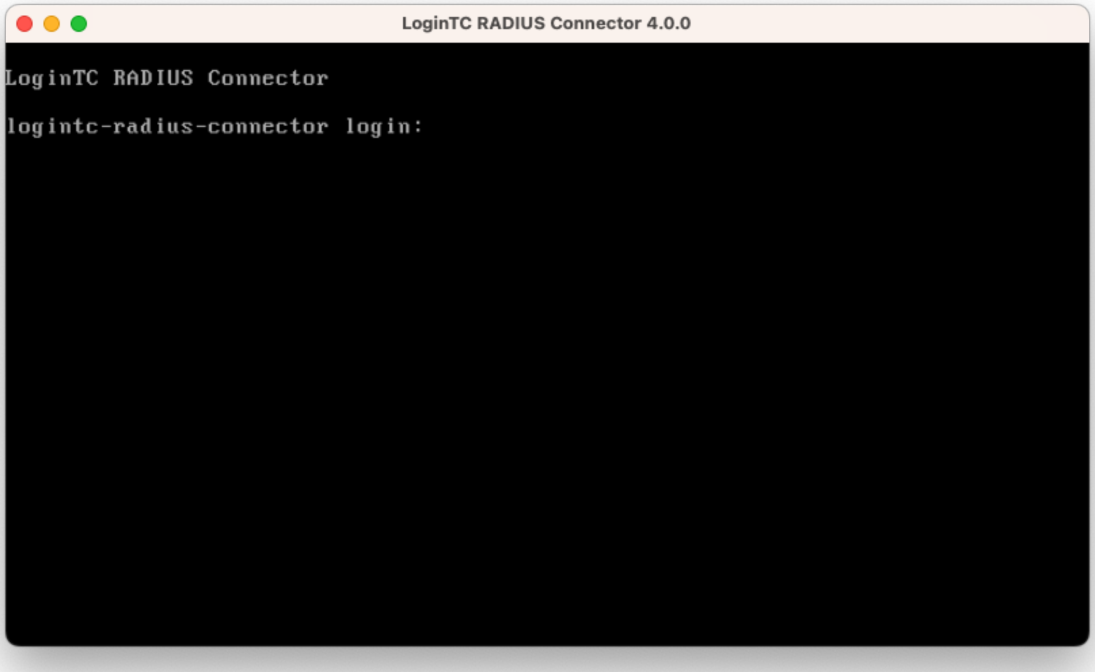
Create a LoginTC Application in LoginTC Admin Panel, follow Create Application Steps.

If you have already created a LoginTC Application for your deployment, then you may skip this section and proceed to Installation.

Installation

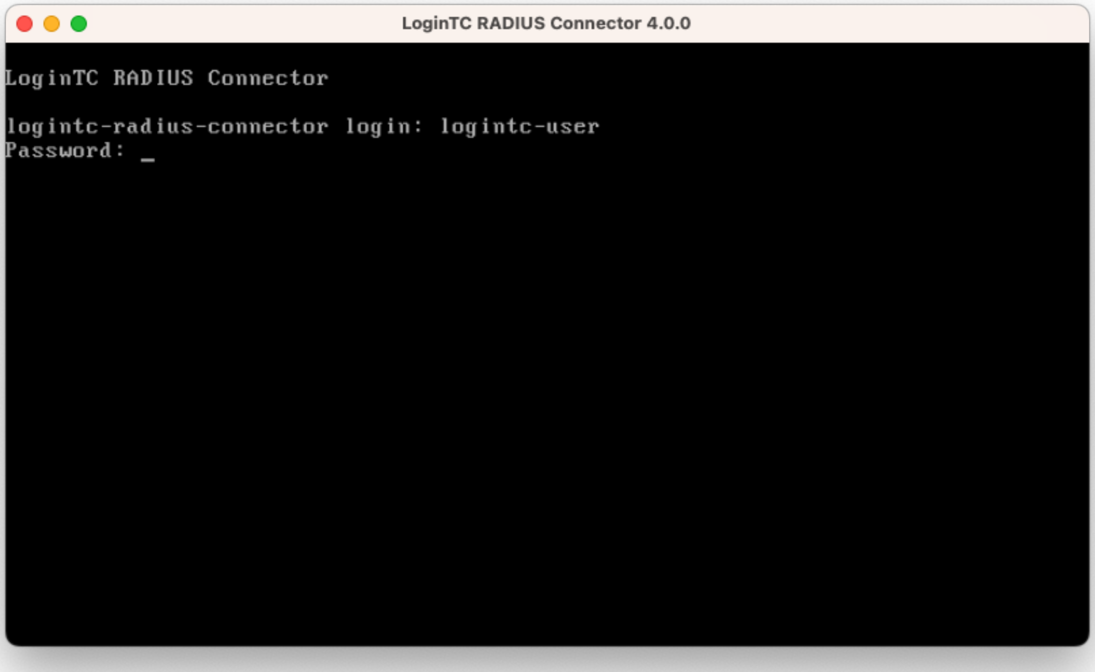
1. Import the virtual appliance your computer virtualization software
   Instructions for Hyper-V
2. Ensure that LoginTC RADIUS CONNECTOR has a virtual network card
3. Start the virtual appliance

4. You will be with a console prompt:



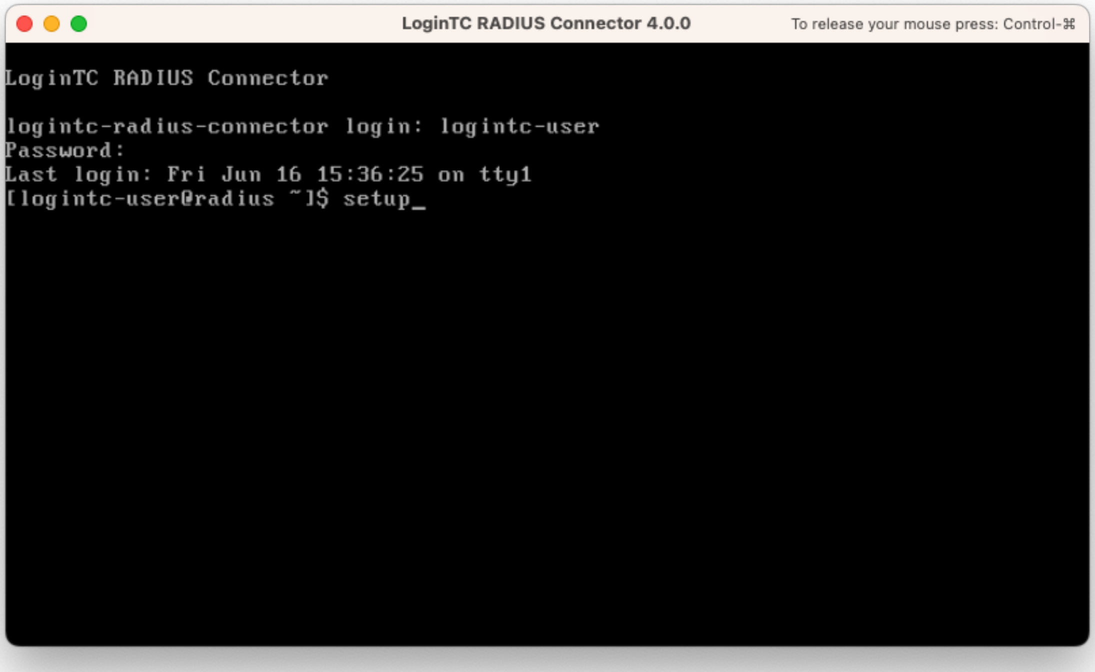
```
LoginTC RADIUS Connector

logintc-radius-connector login:
```

5. Login using the username **logintc-user** and default password **logintcradius**:



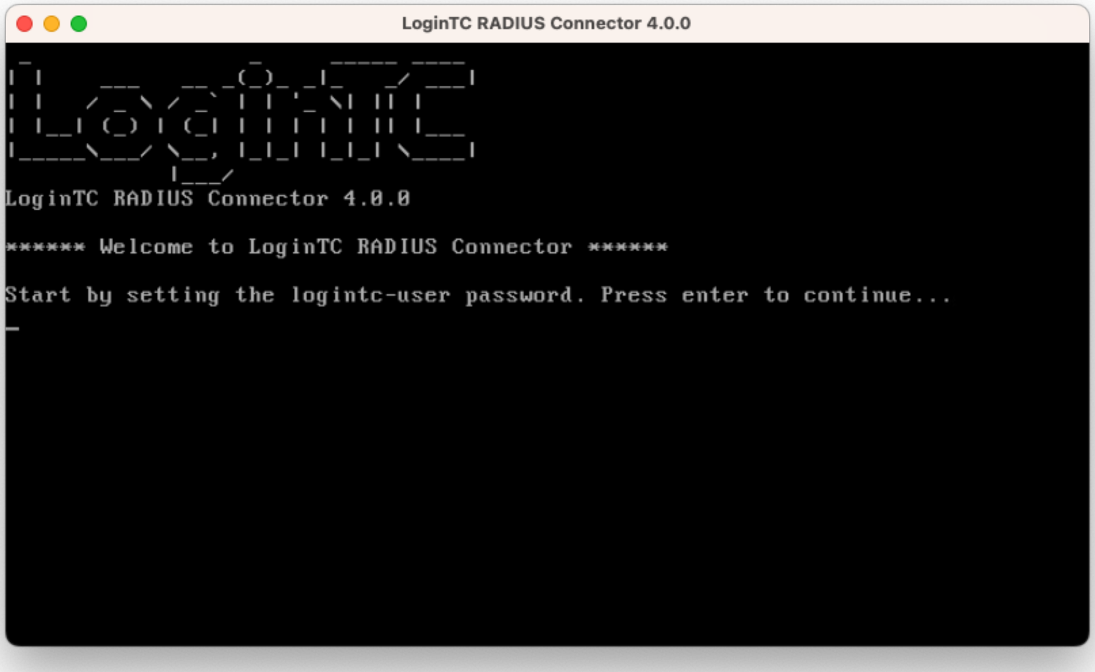
```
LoginTC RADIUS Connector

logintc-radius-connector login: logintc-user
Password: _
```

6. Once logged in type **setup**:


LoginTC RADIUS Connector 4.0.0
To release your mouse press: Control-⌘

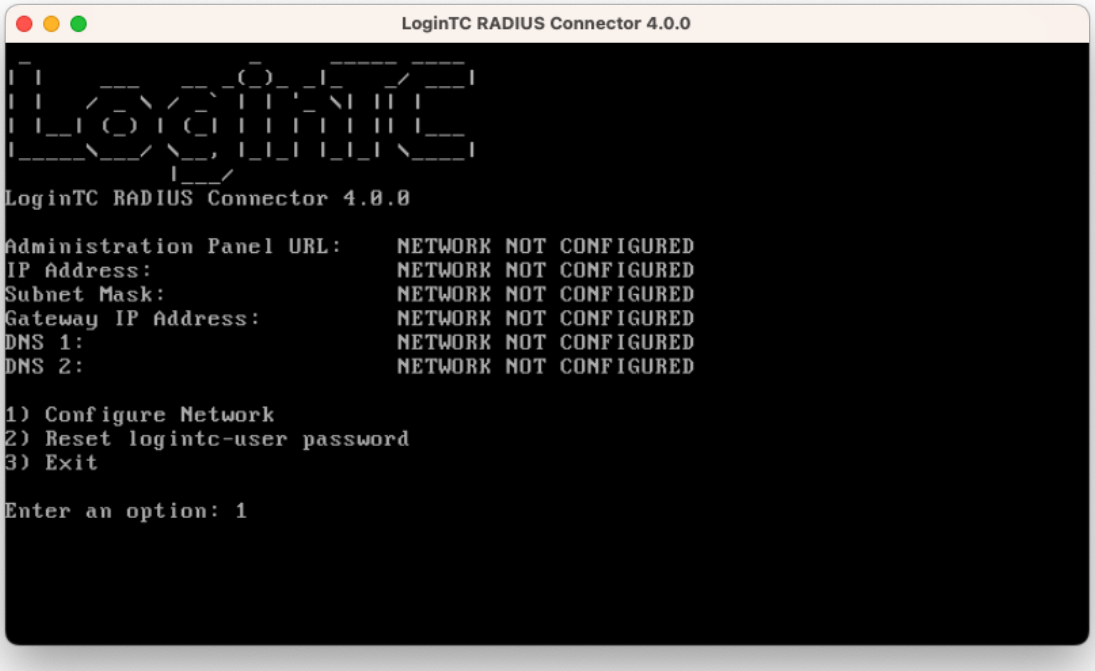
```
LoginTC RADIUS Connector

logintc-radius-connector login: logintc-user
Password:
Last login: Fri Jun 16 15:36:25 on tty1
[logintc-user@radius ~]$ setup_
```

7. Follow the on-screen prompt to setup a new password for **logintc-user**:



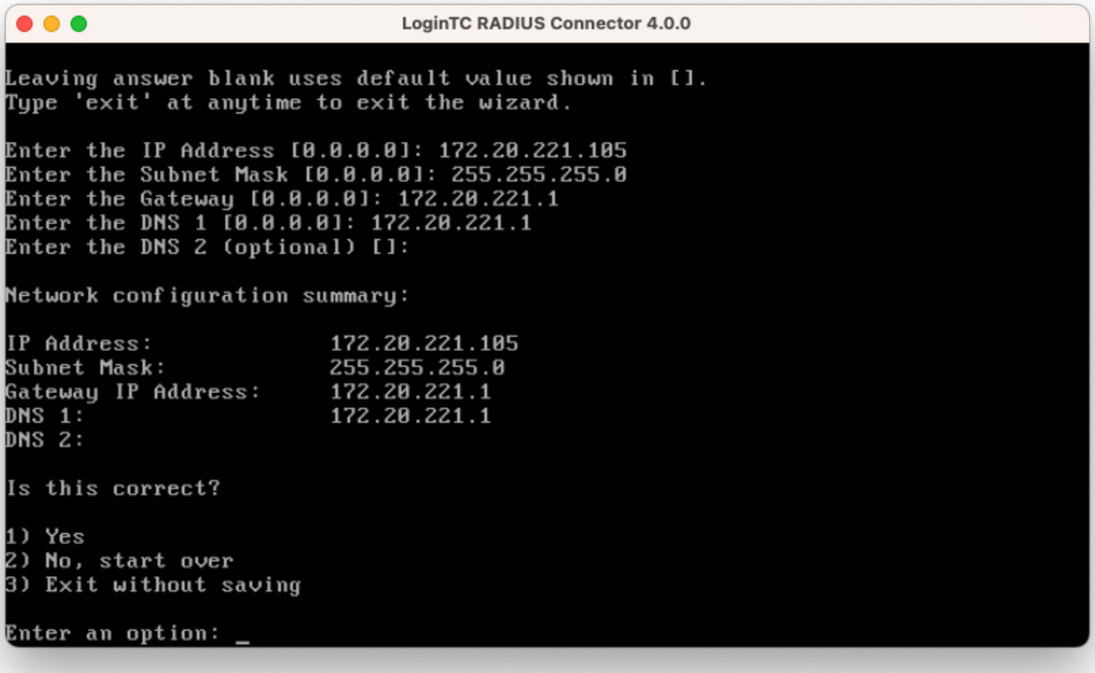
```
 _                _       _____ ____
| |    ___   __ _(_)_ __ |_   _/ ___|
| |   / _ \ / _` | | '_ \  | || |
| |__| (_) | (_| | | | | | | || |___
|_____\___/ \__, |_|_| |_| |_| \____|
            |___/
LoginTC RADIUS Connector 4.0.0

****** Welcome to LoginTC RADIUS Connector ******

Start by setting the logintc-user password. Press enter to continue...
_
```

8. By default the appliance network is not configured. Manually configure the network by typing **1** and hit enter:



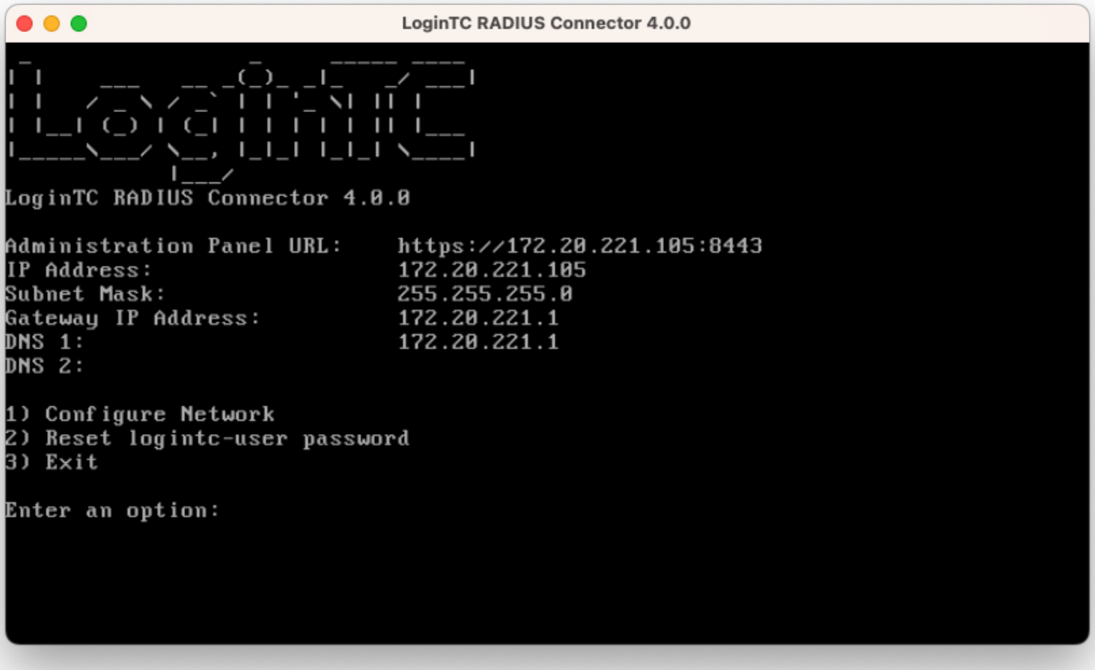
```
 _                _      _____ ____
| |    ___   __ _(_)_ __|_   _/ ___|
| |   / _ \ / _` | | '_ \ | || |
| |__| (_) | (_| | | | | || || |___
|_____\___/ \__, |_|_| |_||_| \____|
            |___/
LoginTC RADIUS Connector 4.0.0

Administration Panel URL:     NETWORK NOT CONFIGURED
IP Address:                   NETWORK NOT CONFIGURED
Subnet Mask:                  NETWORK NOT CONFIGURED
Gateway IP Address:           NETWORK NOT CONFIGURED
DNS 1:                        NETWORK NOT CONFIGURED
DNS 2:                        NETWORK NOT CONFIGURED

1) Configure Network
2) Reset logintc-user password
3) Exit

Enter an option: 1
```

9. Follow the on-screen prompts to setup the network. When done, type **1** and enter to confirm the settings:



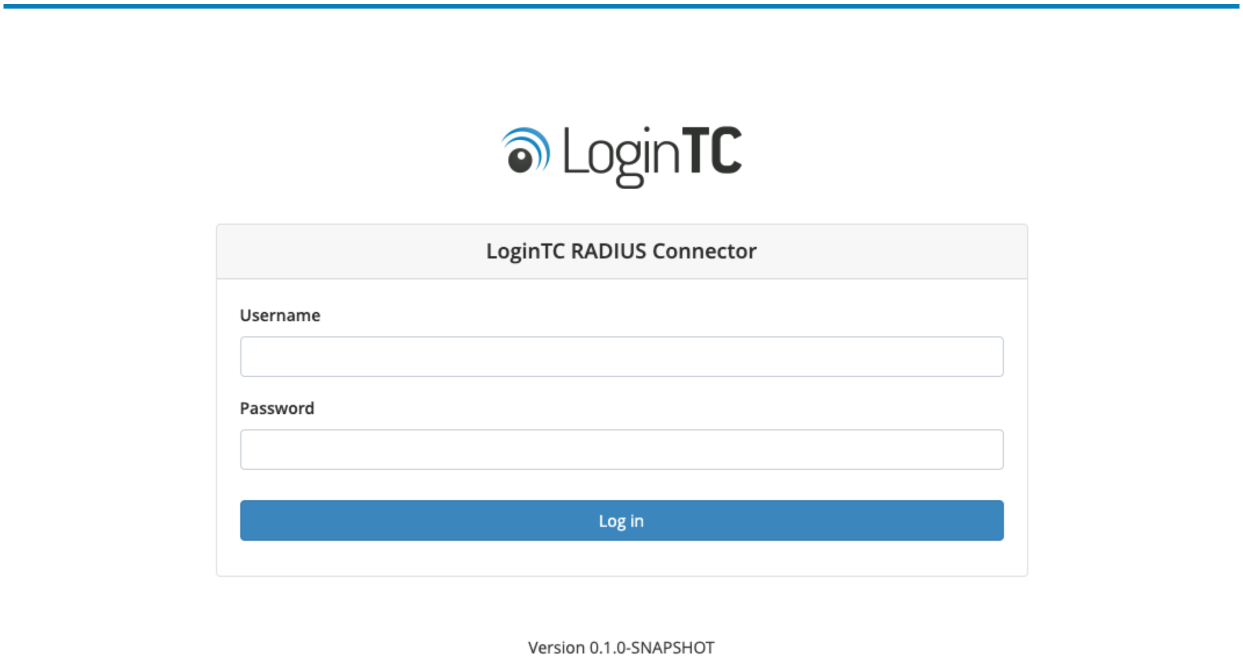
```
Leaving answer blank uses default value shown in [].
Type 'exit' at anytime to exit the wizard.

Enter the IP Address [0.0.0.0]: 172.20.221.105
Enter the Subnet Mask [0.0.0.0]: 255.255.255.0
Enter the Gateway [0.0.0.0]: 172.20.221.1
Enter the DNS 1 [0.0.0.0]: 172.20.221.1
Enter the DNS 2 (optional) []:

Network configuration summary:

IP Address:             172.20.221.105
Subnet Mask:            255.255.255.0
Gateway IP Address:     172.20.221.1
DNS 1:                  172.20.221.1
DNS 2:

Is this correct?

1) Yes
2) No, start over
3) Exit without saving

Enter an option: _
```

10. You will be presented with the network configuration which includes the URL to connect to the appliance from a web browser (example https://172.20.221.105:8443):



```
 _                _       _____ ____
| |    ___   __ _(_)_ __ |_   _/ ___|
| |   / _ \ / _` | | '_ \  | || |
| |__| (_) | (_| | | | | | | || |___
|_____\___/ \__, |_|_| |_| |_| \____|
            |___/
LoginTC RADIUS Connector 4.0.0

Administration Panel URL:    https://172.20.221.105:8443
IP Address:                  172.20.221.105
Subnet Mask:                 255.255.255.0
Gateway IP Address:          172.20.221.1
DNS 1:                       172.20.221.1
DNS 2:

1) Configure Network
2) Reset logintc-user password
3) Exit

Enter an option:
```

11. Navigate to the URL shown in the console dashboard (example: `https://172.20.221.105:8443`):



LoginTC

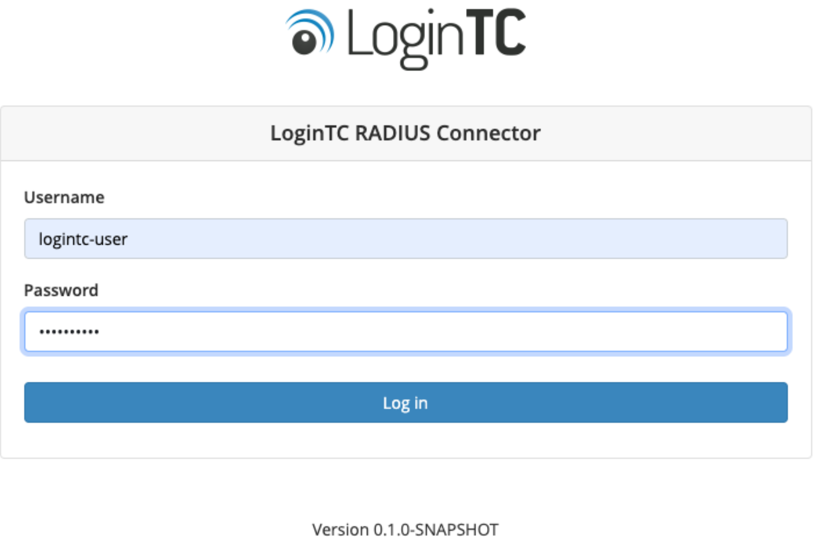
LoginTC RADIUS Connector

Username

Password

Version 0.1.0-SNAPSHOT

12. Login using the username **logintc-user** and the password that was set in the initial setup:



LoginTC RADIUS Connector

Username

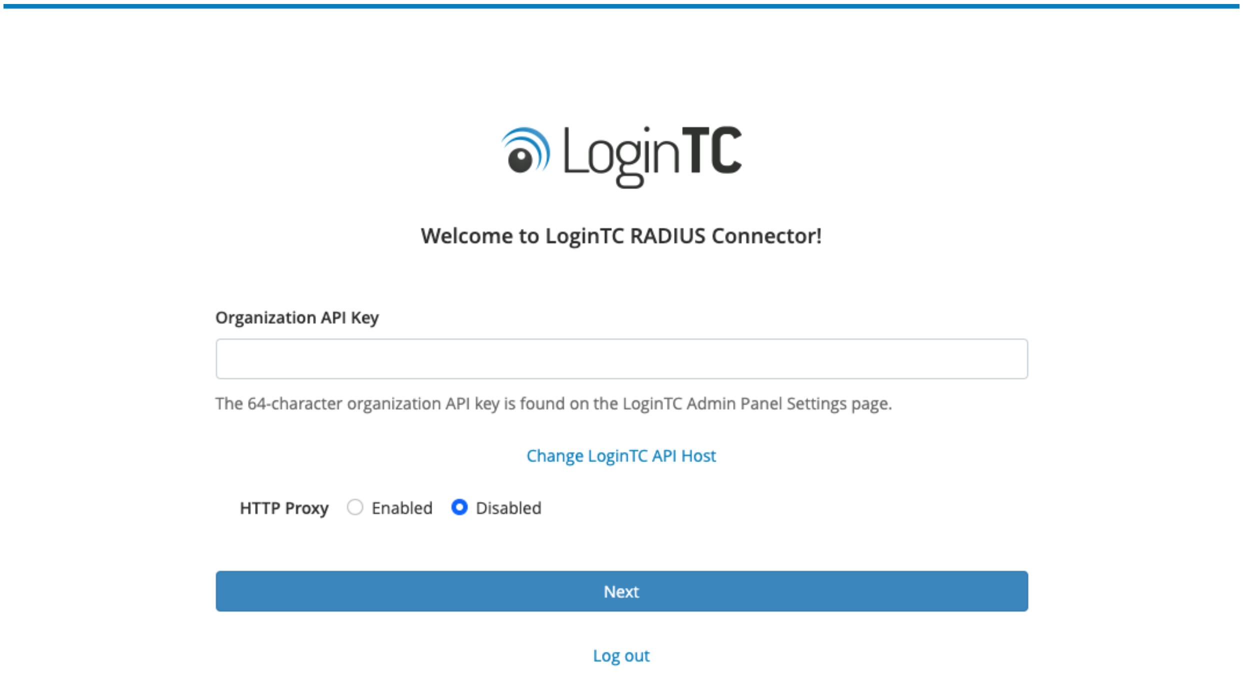
logintc-user

Password

••••••••••

Version 0.1.0-SNAPSHOT

13. Link to your existing LoginTC organization. The 64-character Organization API Key is found on the LoginTC Admin Panel under **Settings** >page **API** >page **Click to view**, also see Organization API Key:



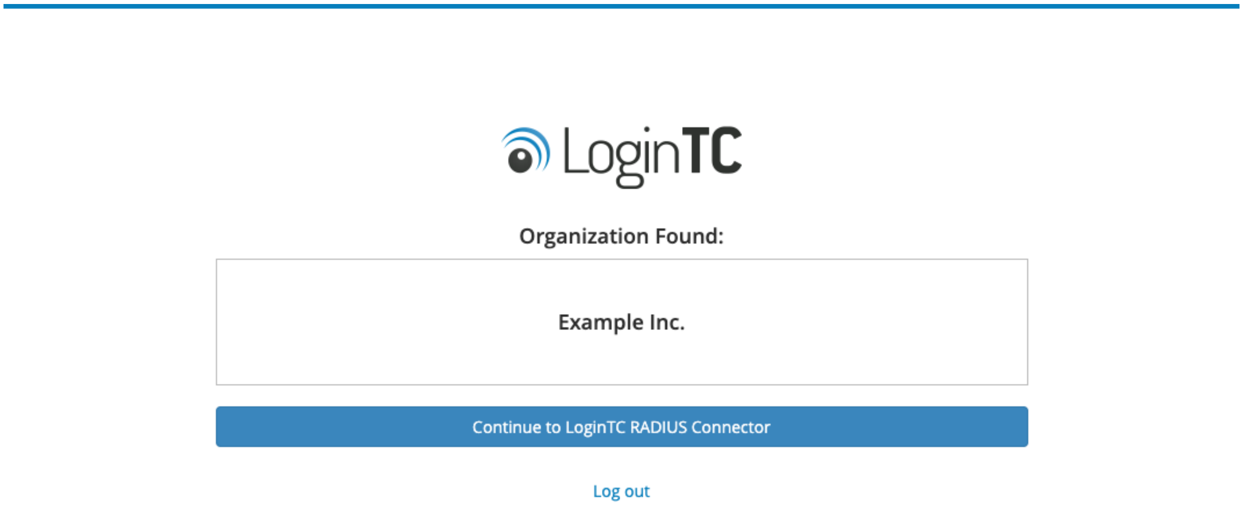
Welcome to LoginTC RADIUS Connector!

Organization API Key

The 64-character organization API key is found on the LoginTC Admin Panel Settings page.

HTTP Proxy ○ Enabled ● Disabled

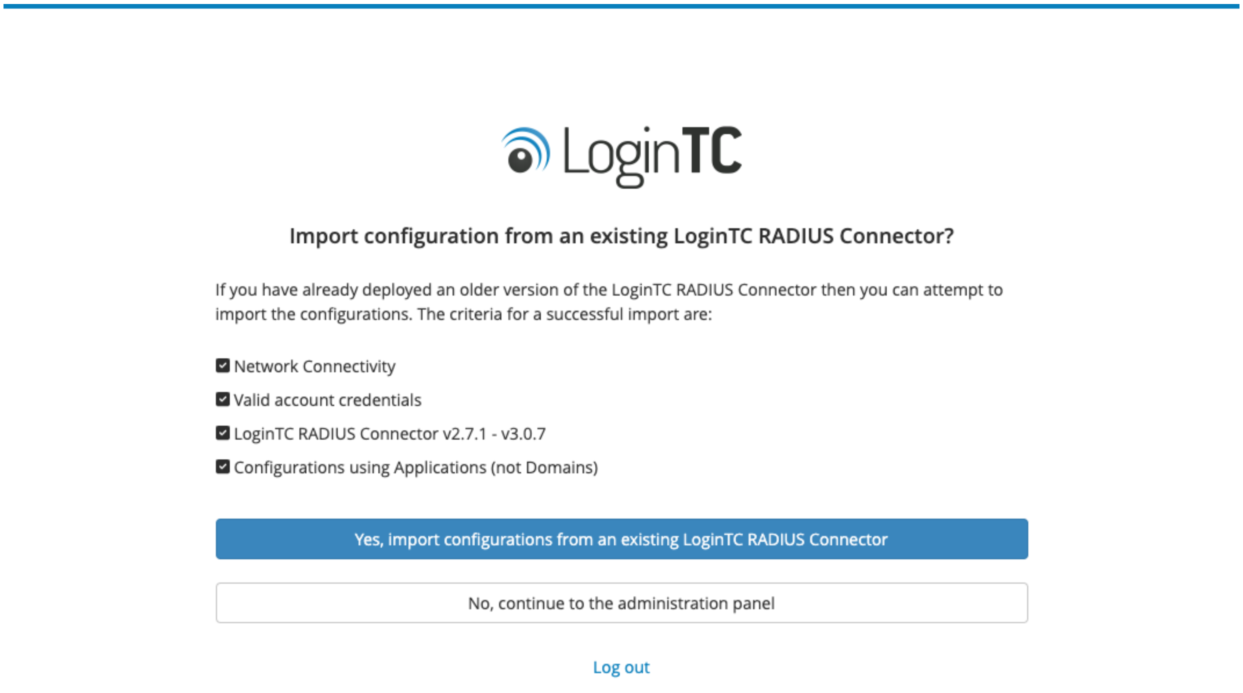
14. Confirm the LoginTC organization name and click **Continue to LoginTC RADIUS Connector**:



Organization Found:

Example Inc.

15. If you have an existing LoginTC RADIUS Connector your wish to import configurations then click **Yes, import configurations from an existing LoginTC RADIUS Connector**, otherwise click **No, continue to the adminsitration panel**:



Import configuration from an existing LoginTC RADIUS Connector?

If you have already deployed an older version of the LoginTC RADIUS Connector then you can attempt to import the configurations. The criteria for a successful import are:

☑ Network Connectivity

☑ Valid account credentials

☑ LoginTC RADIUS Connector v2.7.1 - v3.0.7

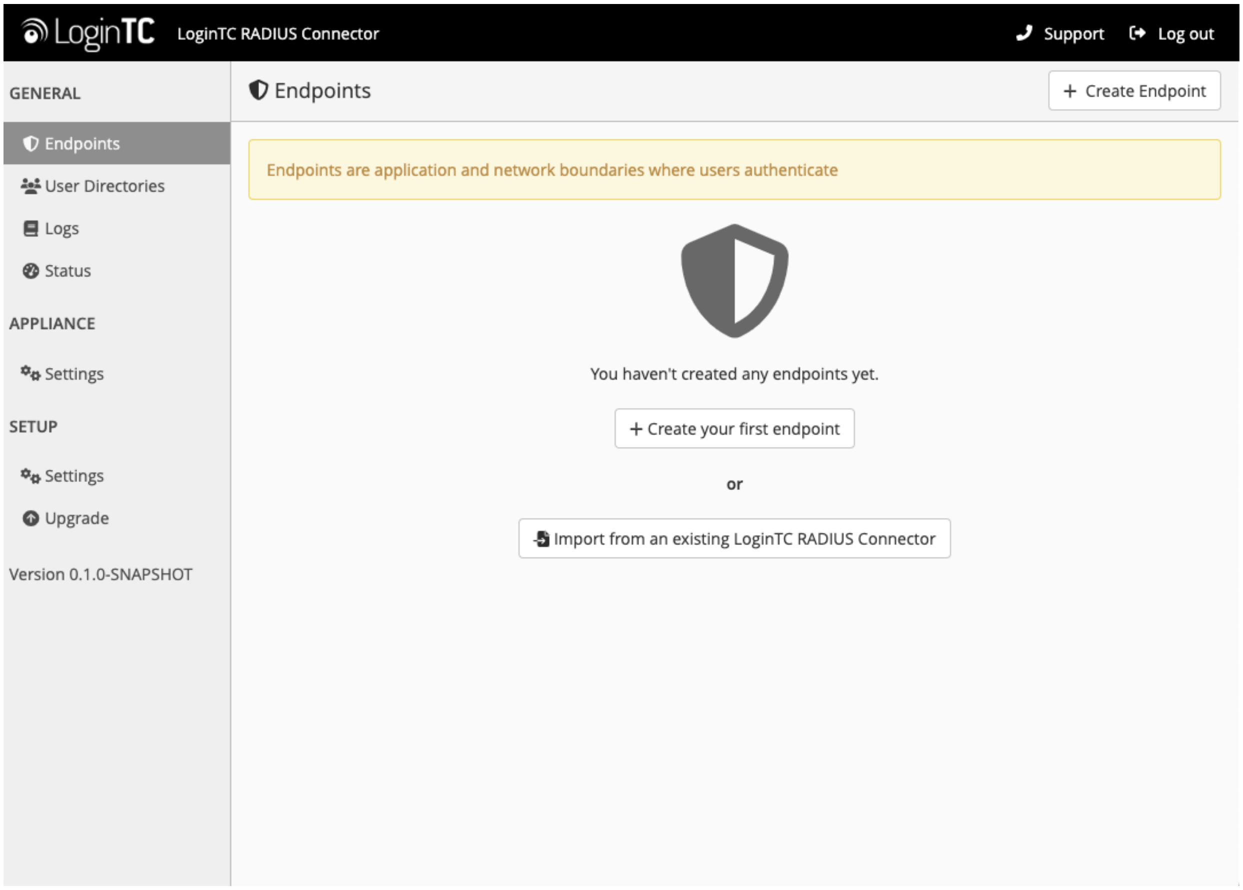
☑ Configurations using Applications (not Domains)

LoginTC
Yes, import configurations from an existing LoginTC RADIUS Connector
No, continue to the administration panel
Log out

NOTE

These instructions assume a new environment. For a complete 2.X / 3.X to 4.X upgrade guide: LoginTC RADIUS Connector Upgrade Guide

16. Now you are ready to use the LoginTC RADIUS Connector:



Endpoints are application and network boundaries where users authenticate

You haven't created any endpoints yet.

The LoginTC RADIUS Connector runs Linux with SELinux. A firewall runs with the following open ports:

Port	Protocol	Purpose
1812	UDP	RADIUS authentication
443	TCP	API traffic
8443	TCP	Web interface
123	UDP	NTP, Clock synchronization (outgoing)

Note: Username and Password `logintc-user` is used for SSH and web access. The default password is `logintcradius`. You will be asked to change the default password on first boot of the appliance.

Configuration for Citrix Two Factor Authentication

Endpoints describe how the appliance will authenticate your RADIUS-speaking device with an optional first factor and LoginTC as a second factor. Each endpoint has **4 Sections**:

1. LoginTC Settings

This section describes how the appliance itself authenticates against LoginTC Admin Panel with your LoginTC Application. Only users that are part of your organization and added to the domain configured will be able to authenticate.

2. User Directory

This section describes how the appliance will conduct an optional first factor. Either against an existing LDAP, Active Directory or RADIUS server. If no first factor is selected, then only LoginTC will be used for authentication.

3. Challenge Strategy / Passthrough

This section describes whether the appliance will perform a LoginTC challenge for an authenticating user. The default is to challenge all users. However with either a static list or Active Directory / LDAP Group you can control whom gets challenged to facilitate seamless testing and rollout.

4. Client Settings

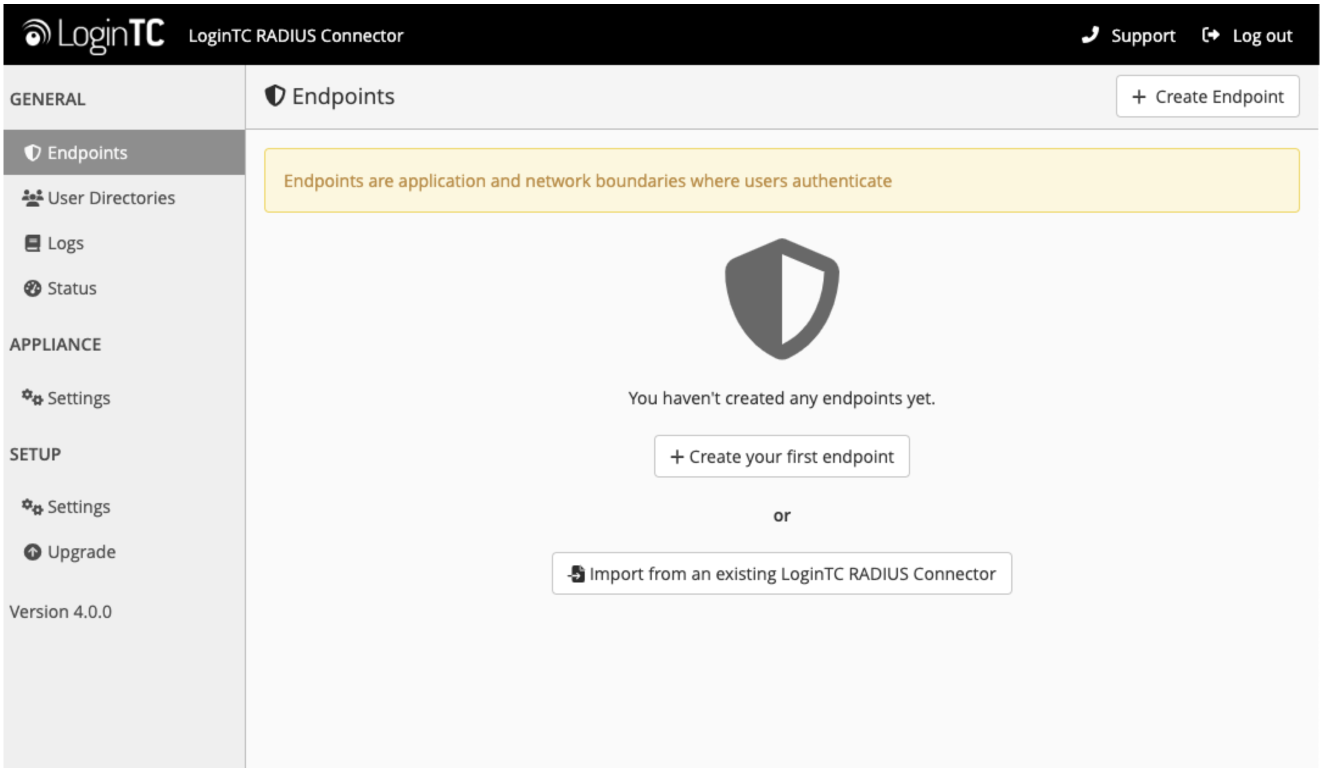
This section describes which RADIUS-speaking device will be connecting to the appliance and whether to encrypt API Key, password and secret parameters.

The **web interface** makes setting up an endpoint simple and straightforward. Each section has a **Test** feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

First Endpoint

Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

Create a new endpoint file by clicking **+ Create your first endpoint**:



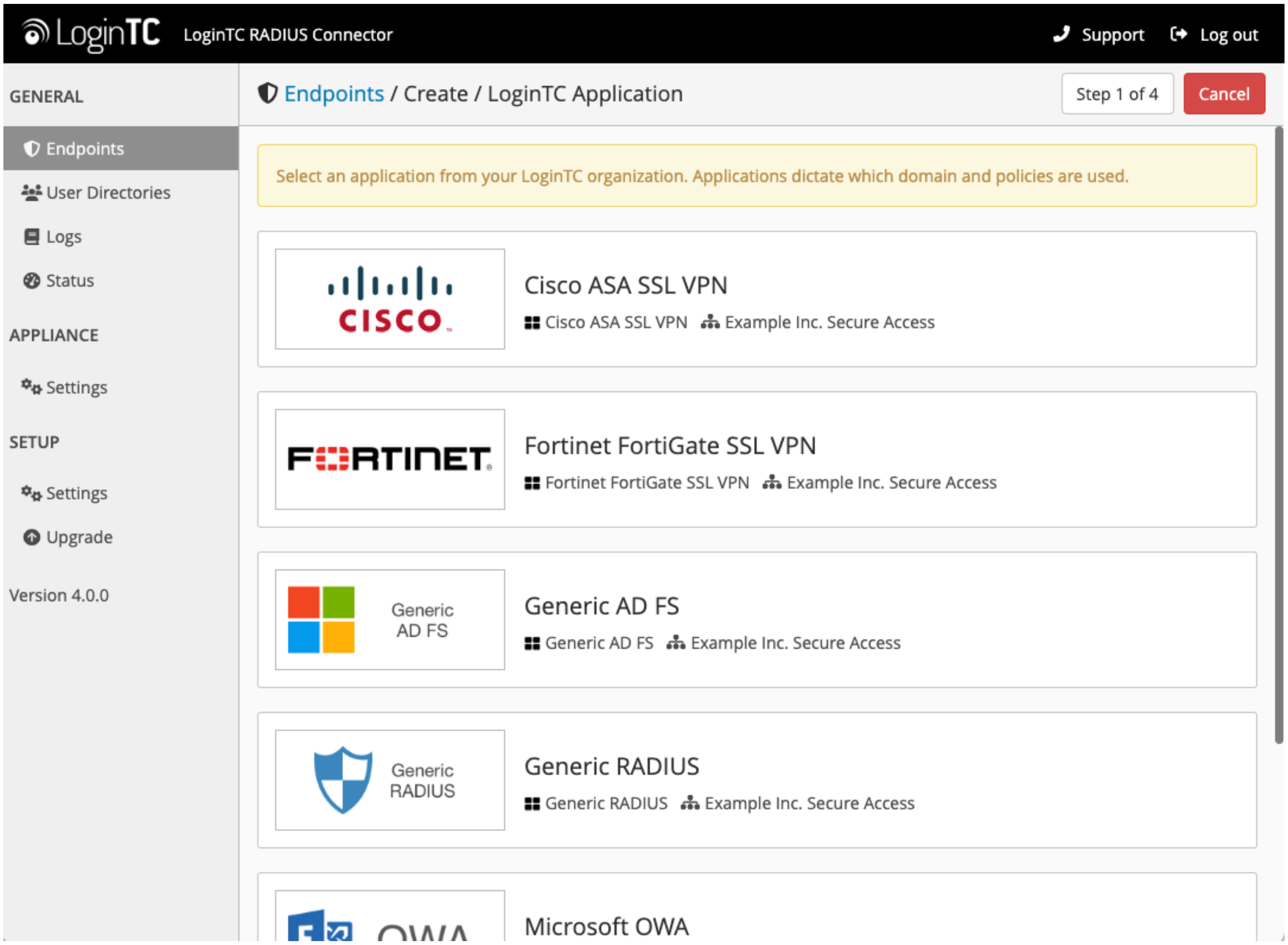
Endpoints are application and network boundaries where users authenticate

You haven't created any endpoints yet.

+ Create your first endpoint
or
Import from an existing LoginTC RADIUS Connector

LoginTC Settings

A list of available Applications will be displayed from your LoginTC organization. Select which LoginTC **Application** to use:



Select an application from your LoginTC organization. Applications dictate which domain and policies are used.

Cisco ASA SSL VPN
Cisco ASA SSL VPN   Example Inc. Secure Access

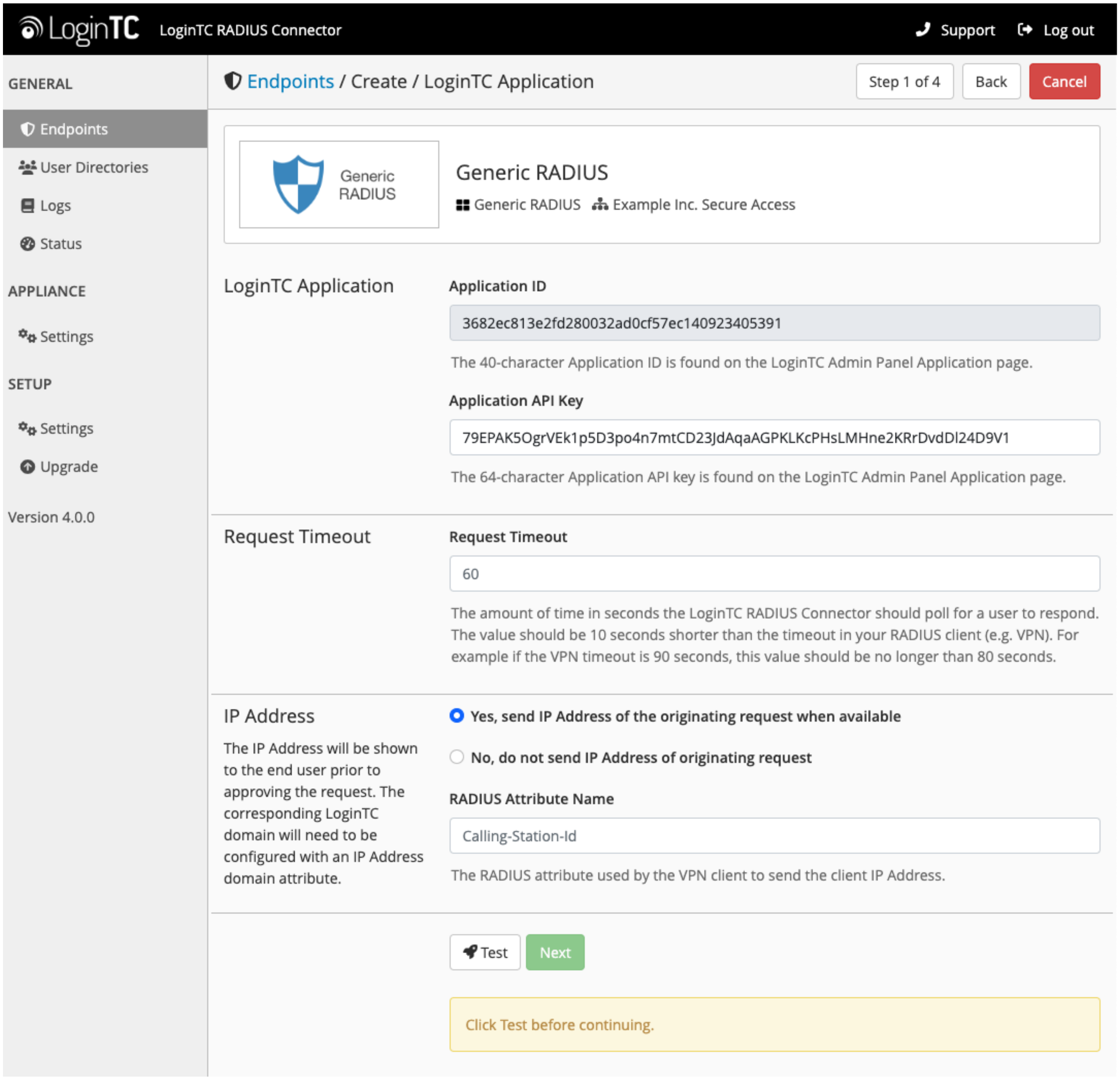
Fortinet FortiGate SSL VPN
Fortinet FortiGate SSL VPN   Example Inc. Secure Access

Generic AD FS
Generic AD FS   Example Inc. Secure Access

Generic RADIUS
Generic RADIUS   Example Inc. Secure Access

Microsoft OWA

Configure the application:



Endpoints / Create / LoginTC Application

Generic RADIUS

Generic RADIUS Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

The 40-character Application ID is found on the LoginTC Admin Panel Application page.

Application API Key

79EPAK5OgrVEk1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDl24D9V1

The 64-character Application API key is found on the LoginTC Admin Panel Application page.

Request Timeout

Request Timeout

60

The amount of time in seconds the LoginTC RADIUS Connector should poll for a user to respond. The value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

IP Address

The IP Address will be shown to the end user prior to approving the request. The corresponding LoginTC domain will need to be configured with an IP Address domain attribute.

● **Yes, send IP Address of the originating request when available**

○ **No, do not send IP Address of originating request**

RADIUS Attribute Name

Calling-Station-Id

The RADIUS attribute used by the VPN client to send the client IP Address.

Click Test before continuing.

Configuration values:

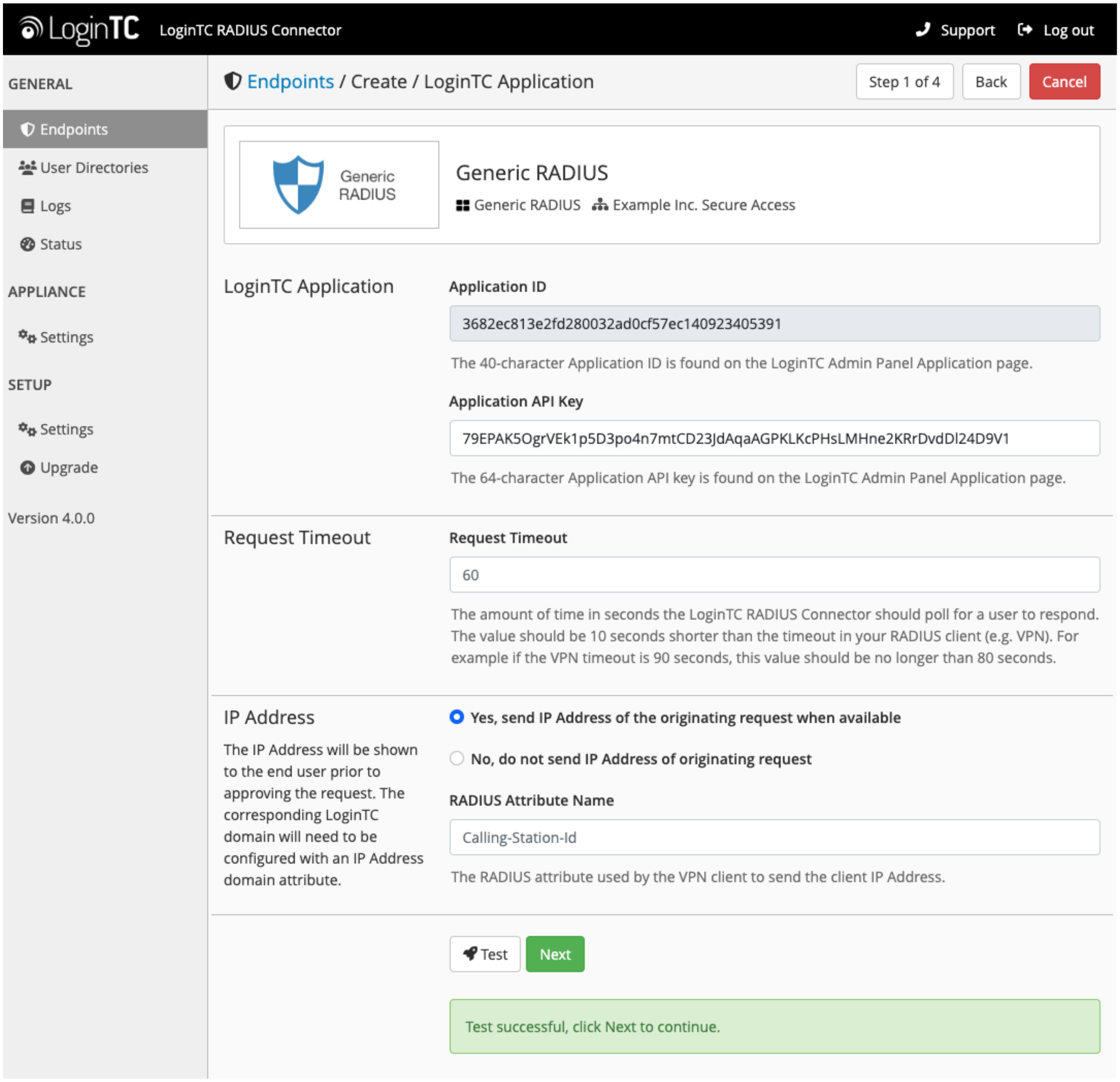
Property	Explanation
`Application ID`	The 40-character Application ID, retrieve Application ID
`Application API Key`	The 64-character Application API Key, retrieve Application API Key
`Request Timeout`	Number of seconds that the RADIUS connector will wait for

The Application ID and Application API Key are found on the LoginTC Admin Panel.

Request Timeout

Make a note of what you set the Request Timeout to as you will need to use a larger timeout value in your RADIUS client. We recommend setting the Request Timeout value to 60 seconds in the LoginTC RADIUS Connector and setting the RADIUS authentication server timeout to 70 seconds in RADIUS Client. For more information see: Recommended settings for an optimal user experience for VPN access

Click **Test** to validate the values and then click **Next**:



Generic RADIUS

Generic RADIUS   Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

The 40-character Application ID is found on the LoginTC Admin Panel Application page.

Application API Key

79EPAK5OgrVEk1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDl24D9V1

The 64-character Application API key is found on the LoginTC Admin Panel Application page.

Request Timeout

Request Timeout

60

The amount of time in seconds the LoginTC RADIUS Connector should poll for a user to respond. The value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

IP Address

The IP Address will be shown to the end user prior to approving the request. The corresponding LoginTC domain will need to be configured with an IP Address domain attribute.

● **Yes, send IP Address of the originating request when available**

○ **No, do not send IP Address of originating request**

RADIUS Attribute Name

Calling-Station-Id

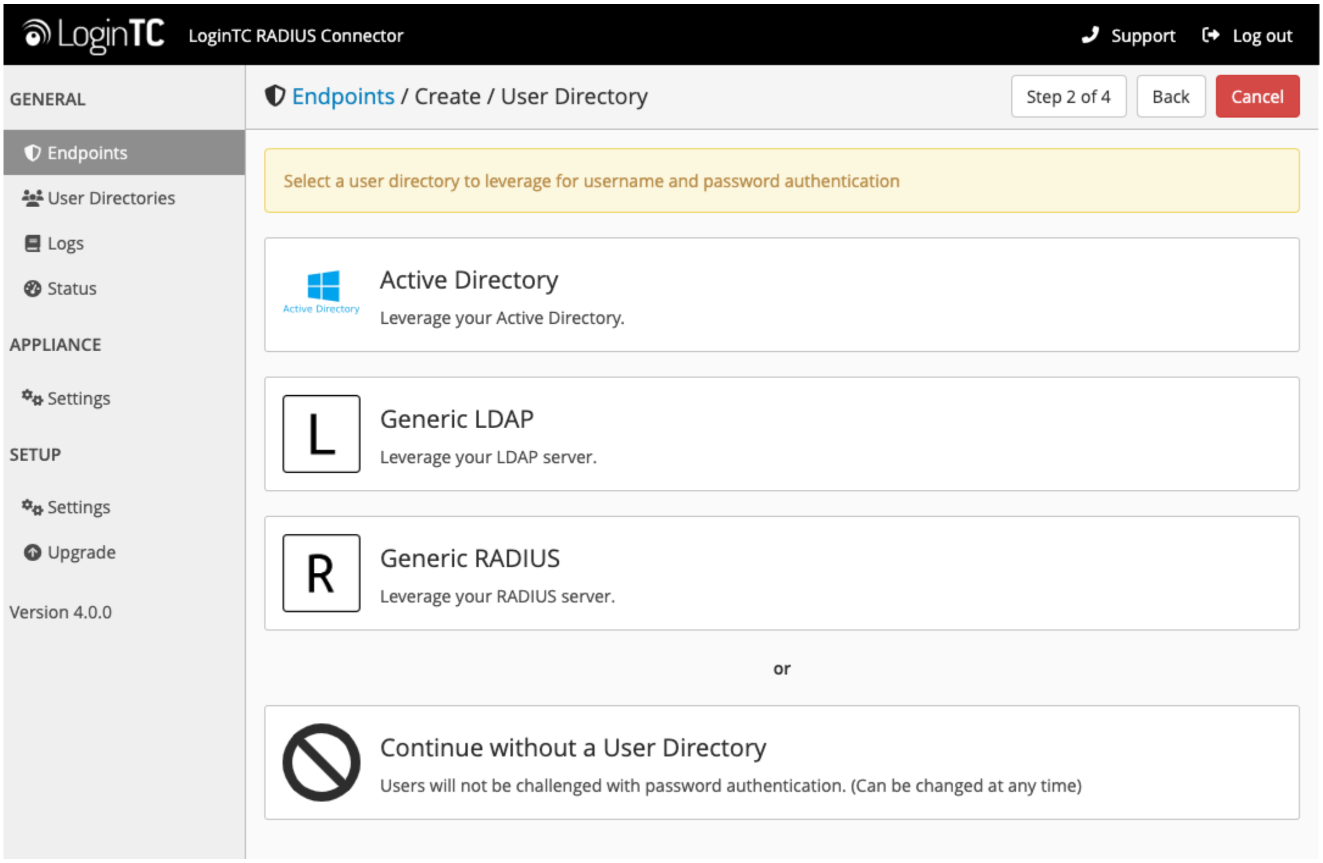
The RADIUS attribute used by the VPN client to send the client IP Address.

Test   Next

Test successful, click Next to continue.

User Directory

Configure the user directory to be used for first authentication factor in conjunction with LoginTC. You may use Active Directory / LDAP or an existing RADIUS server. You may also opt not to use a first factor, in which case LoginTC will be the only authentication factor.



Select a user directory to leverage for username and password authentication

Active Directory
Leverage your Active Directory.

Generic LDAP
Leverage your LDAP server.

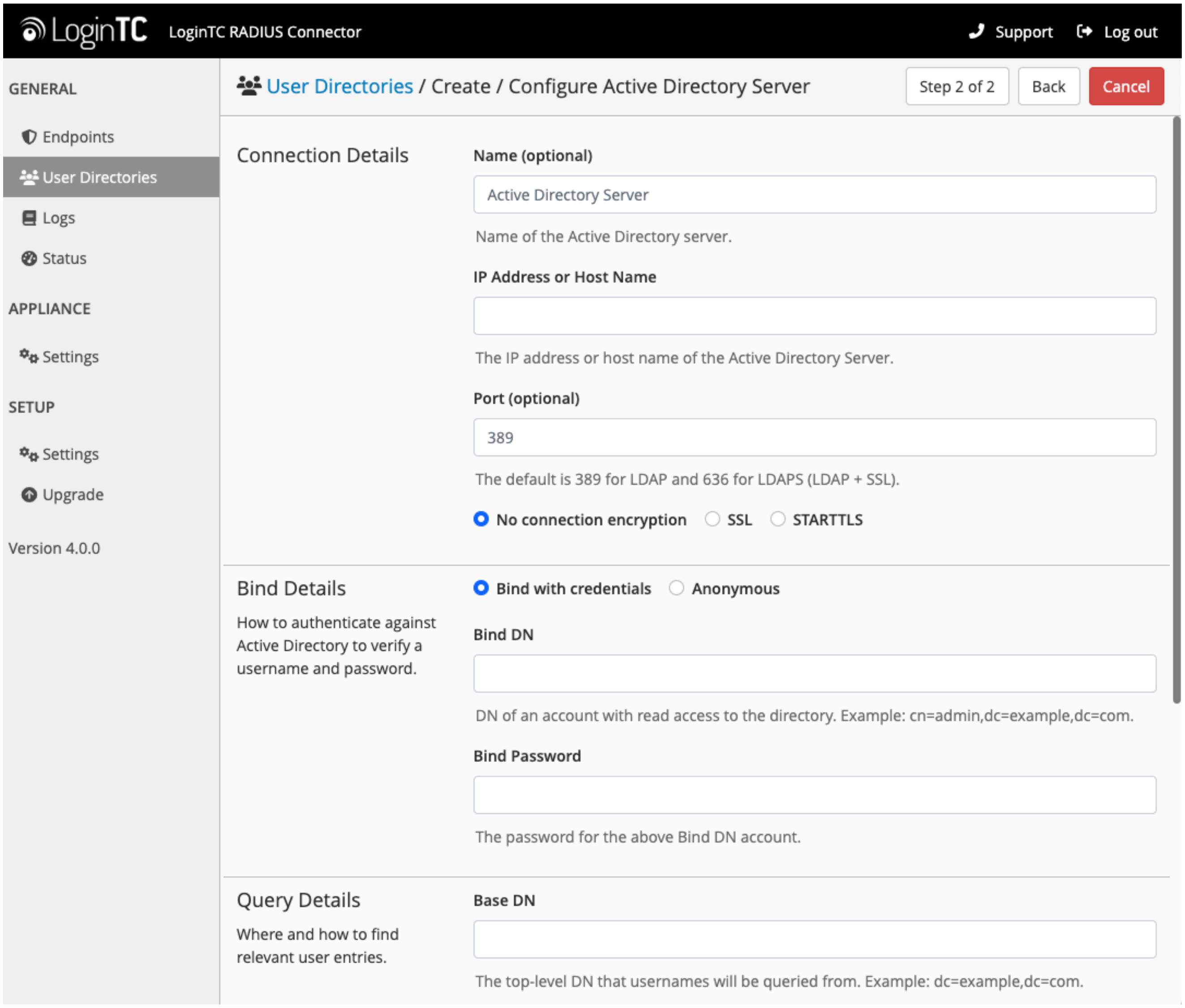
Generic RADIUS
Leverage your RADIUS server.

or

Continue without a User Directory
Users will not be challenged with password authentication. (Can be changed at any time)

Active Directory / Generic LDAP Option

Select **Active Directory** if you have an AD Server. For all other LDAP-speaking directory services, such as OpenDJ or OpenLDAP, select **Generic LDAP**:



Connection Details

Name (optional)

Active Directory Server

Name of the Active Directory server.

IP Address or Host Name

The IP address or host name of the Active Directory Server.

Port (optional)

389

The default is 389 for LDAP and 636 for LDAPS (LDAP + SSL).

● No connection encryption ○ SSL ○ STARTTLS

Bind Details

How to authenticate against Active Directory to verify a username and password.

● Bind with credentials ○ Anonymous

Bind DN

DN of an account with read access to the directory. Example: cn=admin,dc=example,dc=com.

Bind Password

The password for the above Bind DN account.

Query Details

Where and how to find relevant user entries.

Base DN

The top-level DN that usernames will be queried from. Example: dc=example,dc=com.

Configuration values:

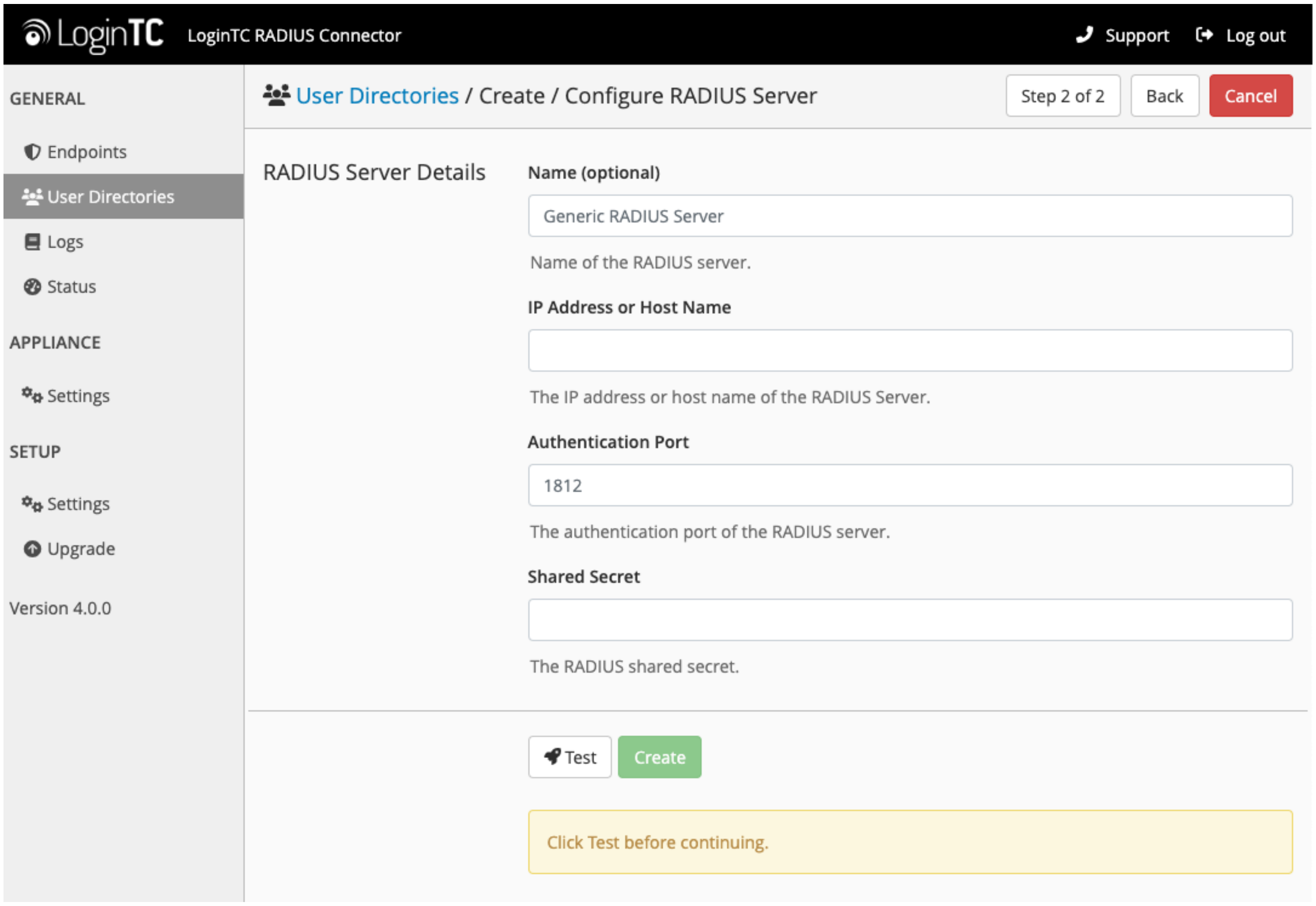
Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389`/`636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The password for the above bind_dn account	`password`
`base_dn`	The top-level DN that you wish to query from	`dc=example,dc=com`

Property	Explanation	Examples
`attr_username`	The attribute containing the user’s username	`sAMAccountName` or `uid`
`attr_name`	The attribute containing the user’s real name	`displayName` or `cn`
`attr_email`	The attribute containing the user’s email address	`mail` or `email`
`LDAP Group` (optional)	The name of the LDAP group to be sent back to the authenticating server.	`SSLVPN-Users`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

Click **Test** to validate the values and then click **Next**.

Existing RADIUS Server Option

If you want to use your existing RADIUS server, select **RADIUS**:



RADIUS Server Details

Name (optional)

Generic RADIUS Server

Name of the RADIUS server.

IP Address or Host Name

The IP address or host name of the RADIUS Server.

Authentication Port

1812

The authentication port of the RADIUS server.

Shared Secret

The RADIUS shared secret.

Click Test before continuing.

Configuration values:

Property	Explanation	Examples
`IP Address or Host Name`	Host or IP address of the RADIUS server	`radius.example.com` or `192.168.1.43`
`Authentication Port` (optional)	Port if the RADIUS server uses non-standard (i.e., `1812`)	`1812`
`Shared Secret`	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	`testing123`

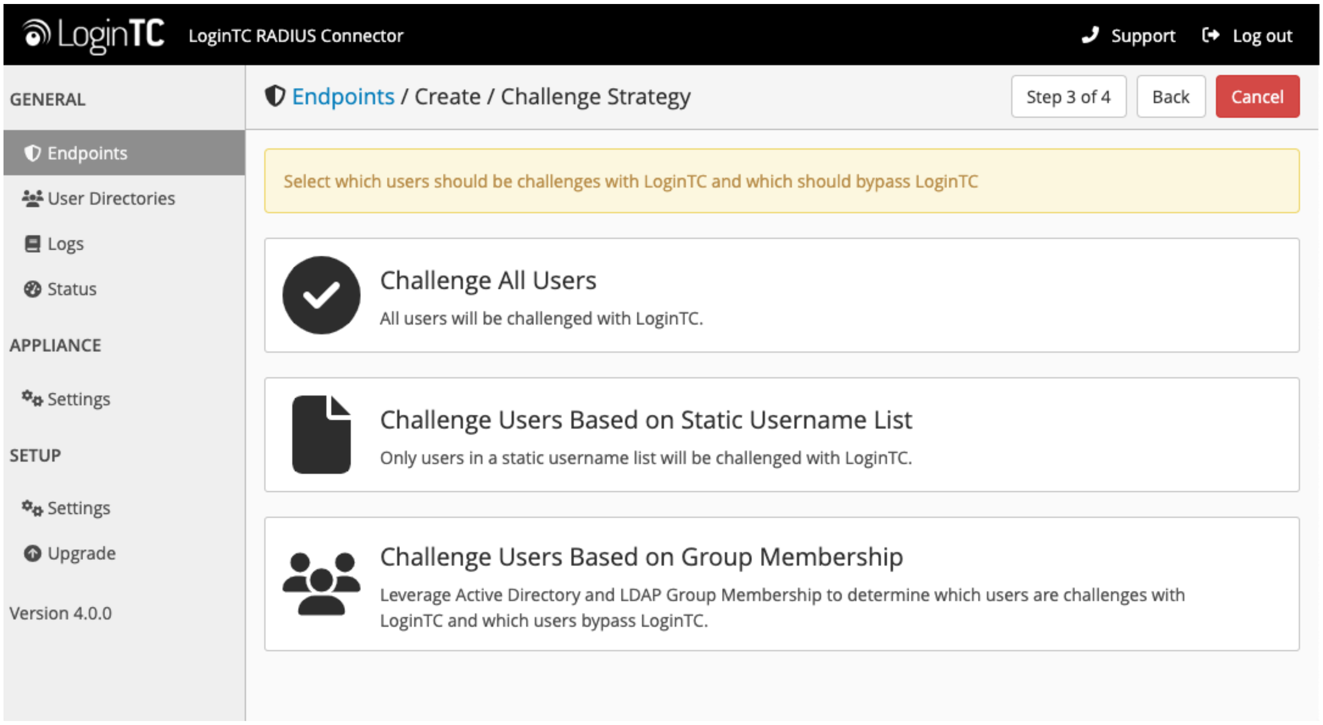
RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) returned by the RADIUS server will be relayed.

Click **Test** to validate the values and then click **Next**.

Challenge Strategy / Passthrough

Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.



Endpoints / Create / Challenge Strategy

Select which users should be challenges with LoginTC and which should bypass LoginTC

Challenge All Users

All users will be challenged with LoginTC.

Challenge Users Based on Static Username List

Only users in a static username list will be challenged with LoginTC.

Challenge Users Based on Group Membership

Leverage Active Directory and LDAP Group Membership to determine which users are challenges with LoginTC and which users bypass LoginTC.

For example, with smaller or proof of concept deployments select the Static List option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured First Authentication Factor. That means you will be able to test LoginTC without affecting existing users accessing your VPN.

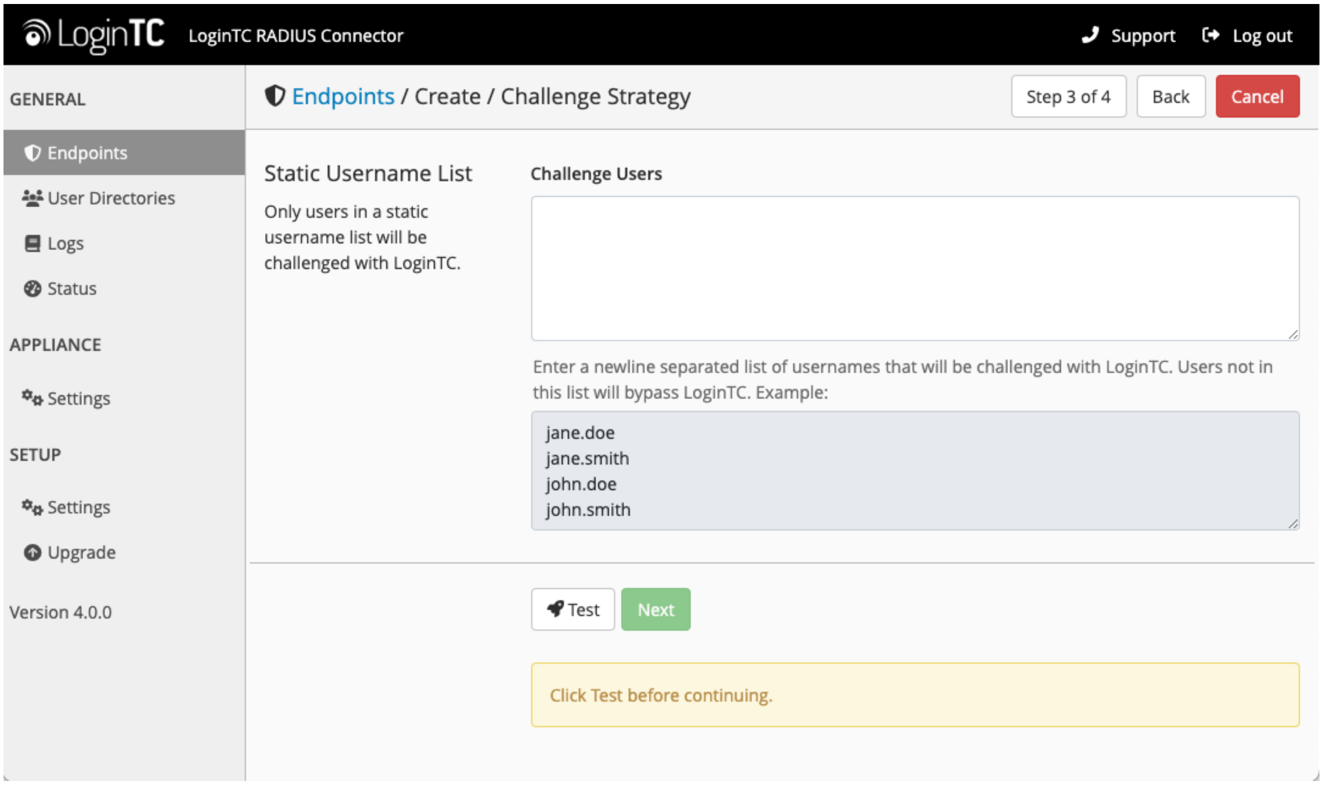
For larger deployments you can elect to use the Active Directory or LDAP Group option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC your LDAP and Active Directory group policy will ensure that they will be challenged with LoginTC. Users not part of the group will only be challenged with the configured First Authentication Factor.

Challenge All Users

Select this option if you wish every user to be challenged with LoginTC.

Challenge Users Based on Static Username List

Select this option if you wish to have a static list of users that will be challenged with LoginTC. Good for small number of users.



Static Username List

Only users in a static username list will be challenged with LoginTC.

Challenge Users

Enter a newline separated list of usernames that will be challenged with LoginTC. Users not in this list will bypass LoginTC. Example:

```
jane.doe
jane.smith
john.doe
john.smith
```

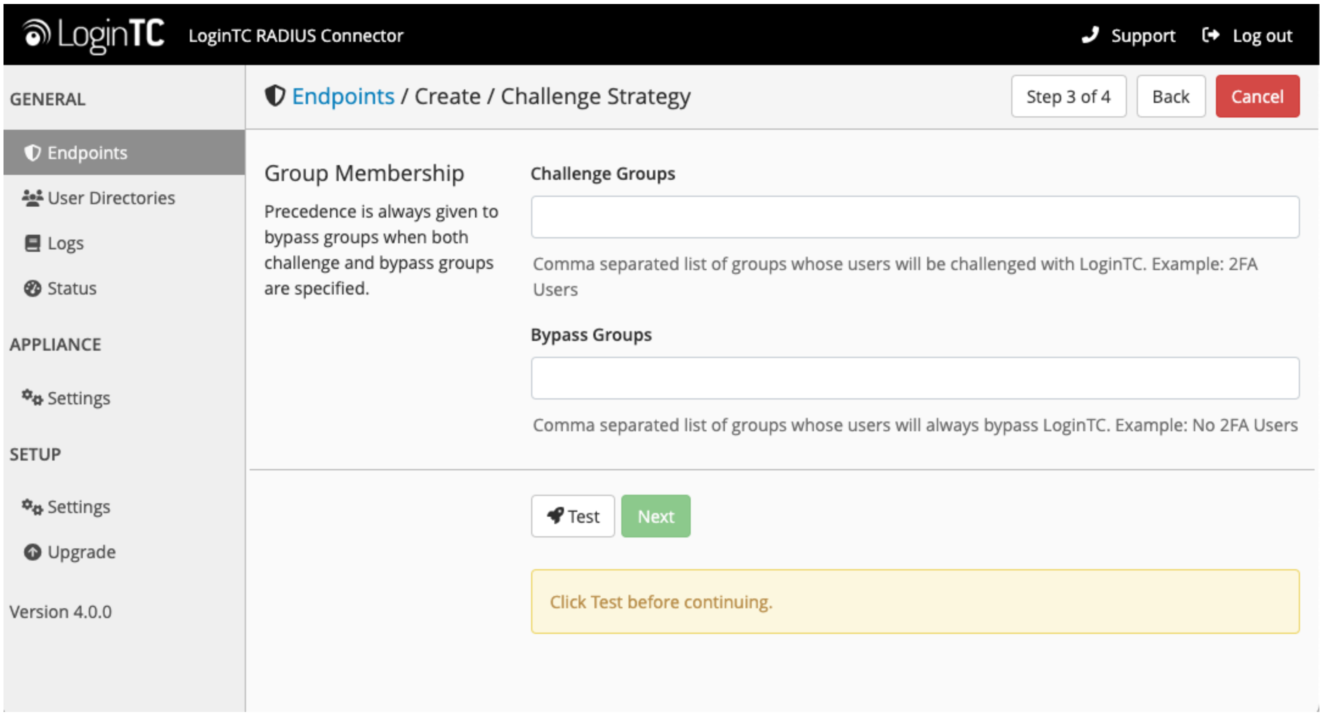
Click Test before continuing.

LoginTC challenge users: a new line separated list of usernames. For example:

```
jane.doe
jane.smith
john.doe
john.smith
```

Challenge Users Based on Group Membership

Select this option if you wish to have only users part of a particular Active Directory or LDAP group to be challenged with LoginTC. Good for medium and large number of users.



Endpoints / Create / Challenge Strategy

Group Membership

Precedence is always given to bypass groups when both challenge and bypass groups are specified.

Challenge Groups

Comma separated list of groups whose users will be challenged with LoginTC. Example: 2FA Users

Bypass Groups

Comma separated list of groups whose users will always bypass LoginTC. Example: No 2FA Users

Click Test before continuing.

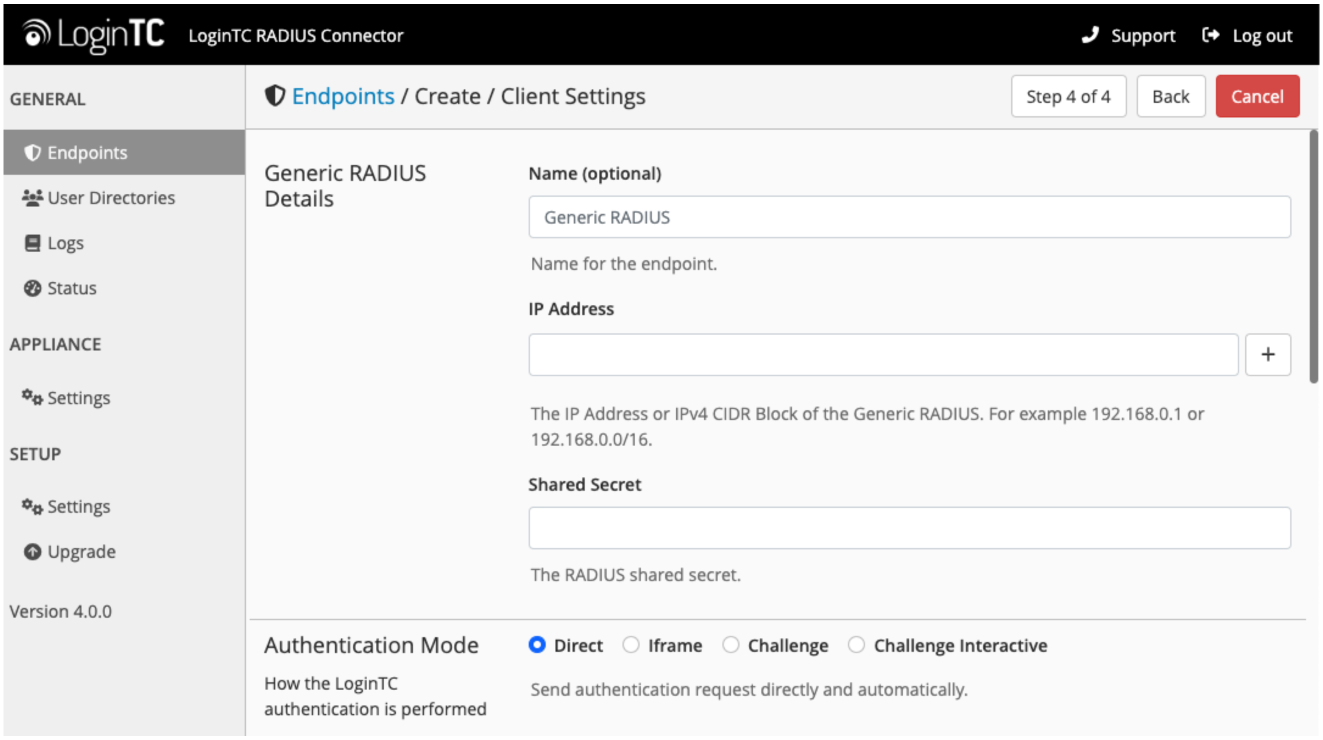
Configuration values:

Property	Explanation	Examples
`Challenge Groups (Optional)`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users` or `two-factor-users`
`Challenge Groups (Optional)`	Comma separated list of groups for which users will always bypass LoginTC	`NOMFA-Users`

Click **Test** to validate the values and then click **Next**.

Client Settings

Configure RADIUS client (e.g. your RADIUS-speaking VPN):



Generic RADIUS Details

Name (optional)

Generic RADIUS

Name for the endpoint.

IP Address

The IP Address or IPv4 CIDR Block of the Generic RADIUS. For example 192.168.0.1 or 192.168.0.0/16.

Shared Secret

The RADIUS shared secret.

Authentication Mode

How the LoginTC authentication is performed

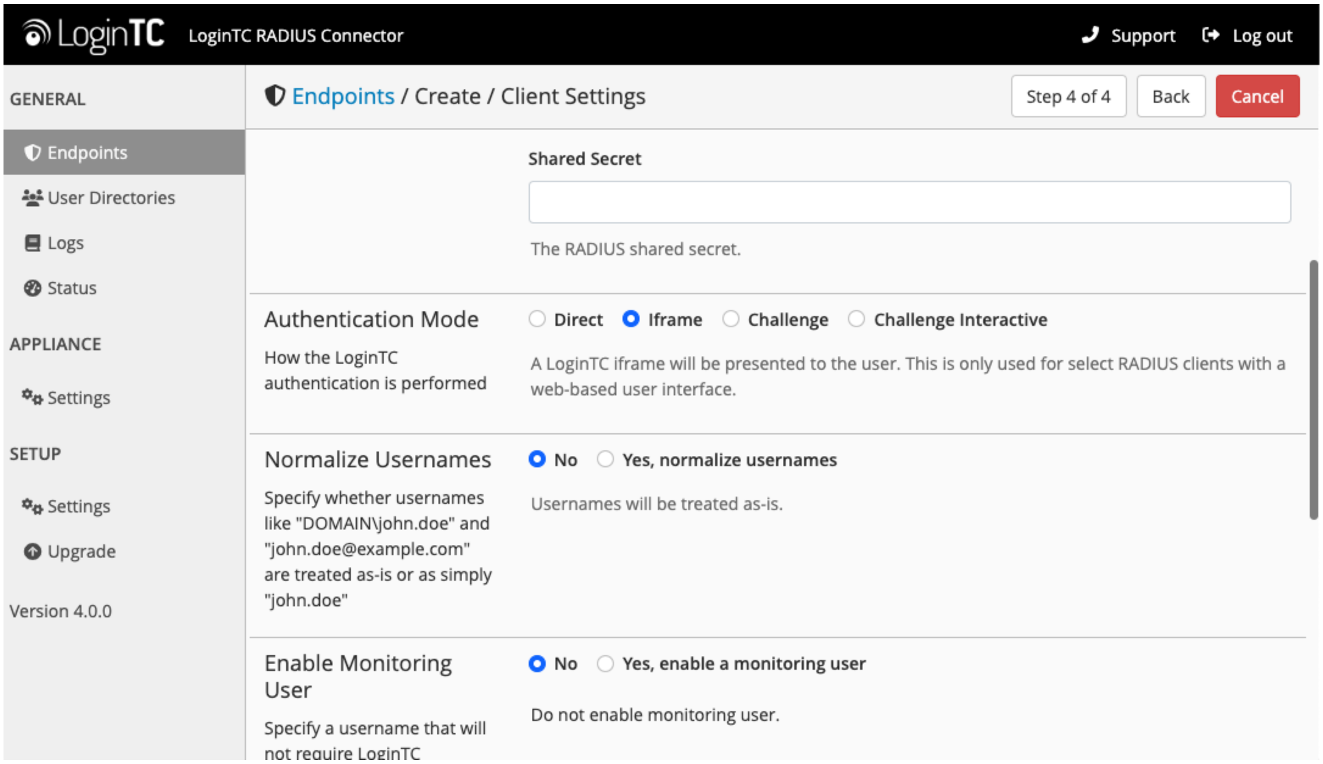
● Direct ○ Iframe ○ Challenge ○ Challenge Interactive

Send authentication request directly and automatically.

Client configuration values:

Property	Explanation	Examples
`name`	A unique identifier of your RADIUS client	`CorporateVPN`
`IP Addresss`	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN). Add additional IP Addresses by clicking **plus**.	`192.168.1.44`
`Shared Secret`	The secret shared between the LoginTC RADIUS Connector and its client	`bigsecret`

Under Authentication Mode select **Iframe**



Endpoints / Create / Client Settings

Shared Secret

The RADIUS shared secret.

Authentication Mode

How the LoginTC authentication is performed

○ Direct ● Iframe ○ Challenge ○ Challenge Interactive

A LoginTC iframe will be presented to the user. This is only used for select RADIUS clients with a web-based user interface.

Normalize Usernames

Specify whether usernames like "DOMAIN\john.doe" and "john.doe@example.com" are treated as-is or as simply "john.doe"

● No ○ Yes, normalize usernames

Usernames will be treated as-is.

Enable Monitoring User

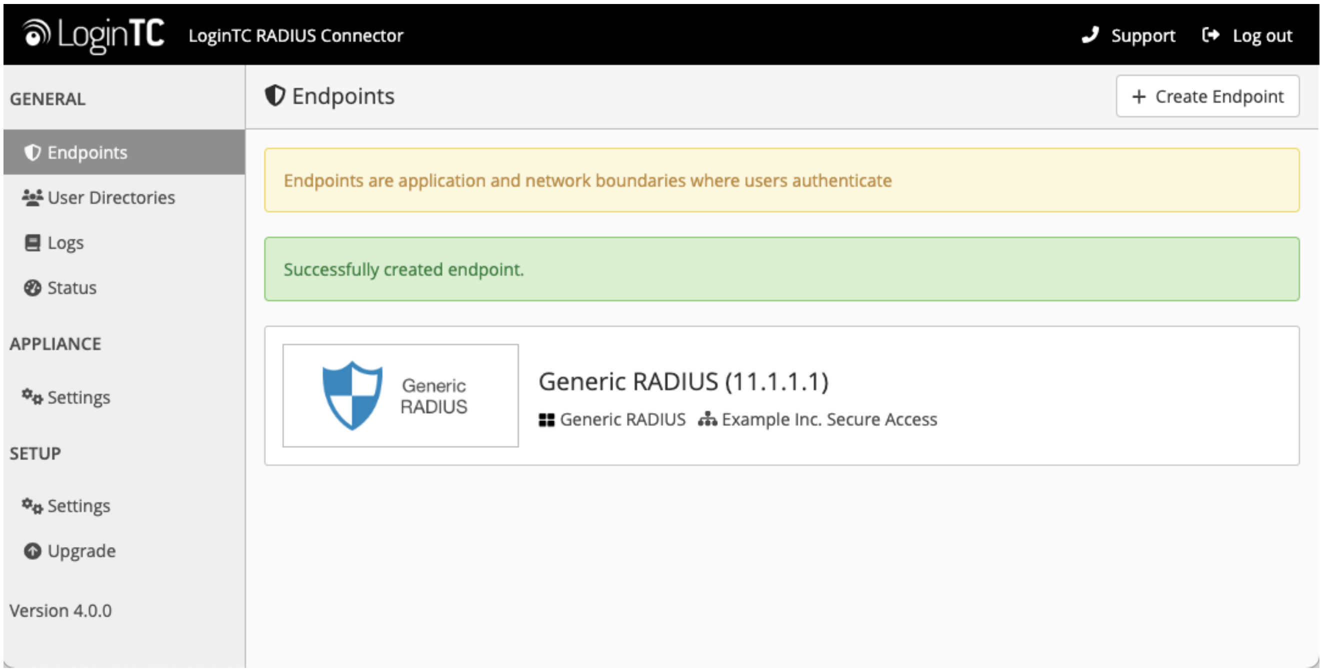
Specify a username that will not require LoginTC

● No ○ Yes, enable a monitoring user

Do not enable monitoring user.

The user will be prompted on how they wish to proceed with second-factor authentication (e.g. LoginTC Push, OTP, bypass code). Your RADIUS client must support RADIUS challenges to use this. Challenging the user will often result in a better user experience. See User Experience for more information.

Click **Test** to validate the values and then click **Save**.



Endpoints

Endpoints are application and network boundaries where users authenticate

Successfully created endpoint.

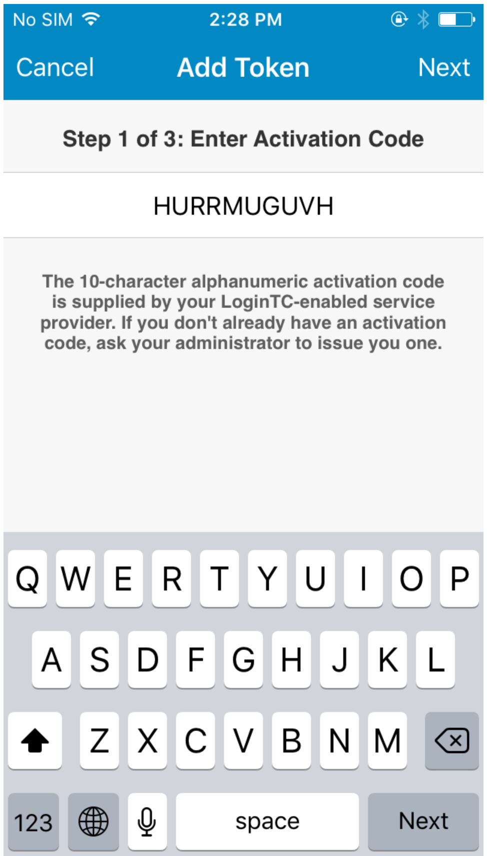
Generic RADIUS (11.1.1.1)

Generic RADIUS Example Inc. Secure Access

Testing

When you are ready to test your configuration, create a LoginTC user (if you haven't already done so). The username should match your existing user. Provision a token by following the steps:

1. In a new tab / window log into the LoginTC Admin Panel
2. Click **Domains**
3. Click on your domain
4. Click on **Members**
5. Click **Issue Token** button beside your user:
6. A 10-character alphanumeric activation code will appear beside the user:
7. Open the LoginTC mobile app.
8. Enter the 10-character alphanumeric activation code:

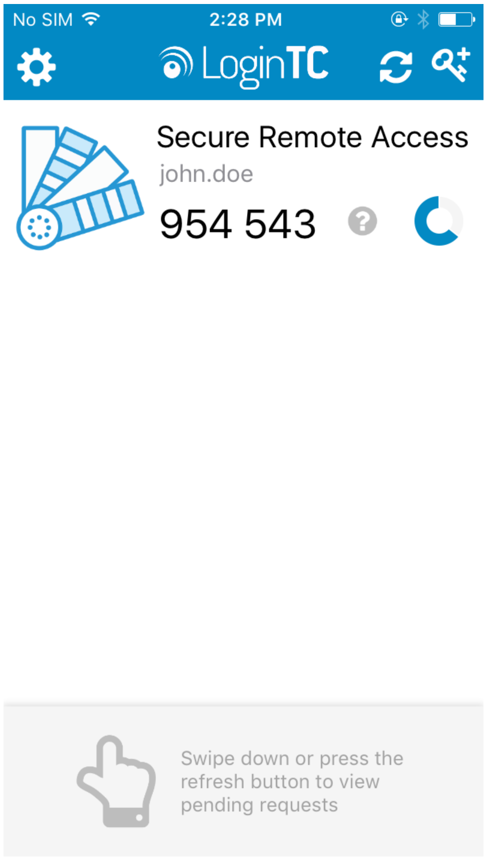


Step 1 of 3: Enter Activation Code

HURRMUGUVH

The 10-character alphanumeric activation code is supplied by your LoginTC-enabled service provider. If you don't already have an activation code, ask your administrator to issue you one.

9. Load the token to complete the process



Secure Remote Access

john.doe

954 543

Swipe down or press the refresh button to view pending requests

When you have loaded a token for your new user and domain, navigate to your appliance **web interface** URL:

Click **Test Configuration**:

Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

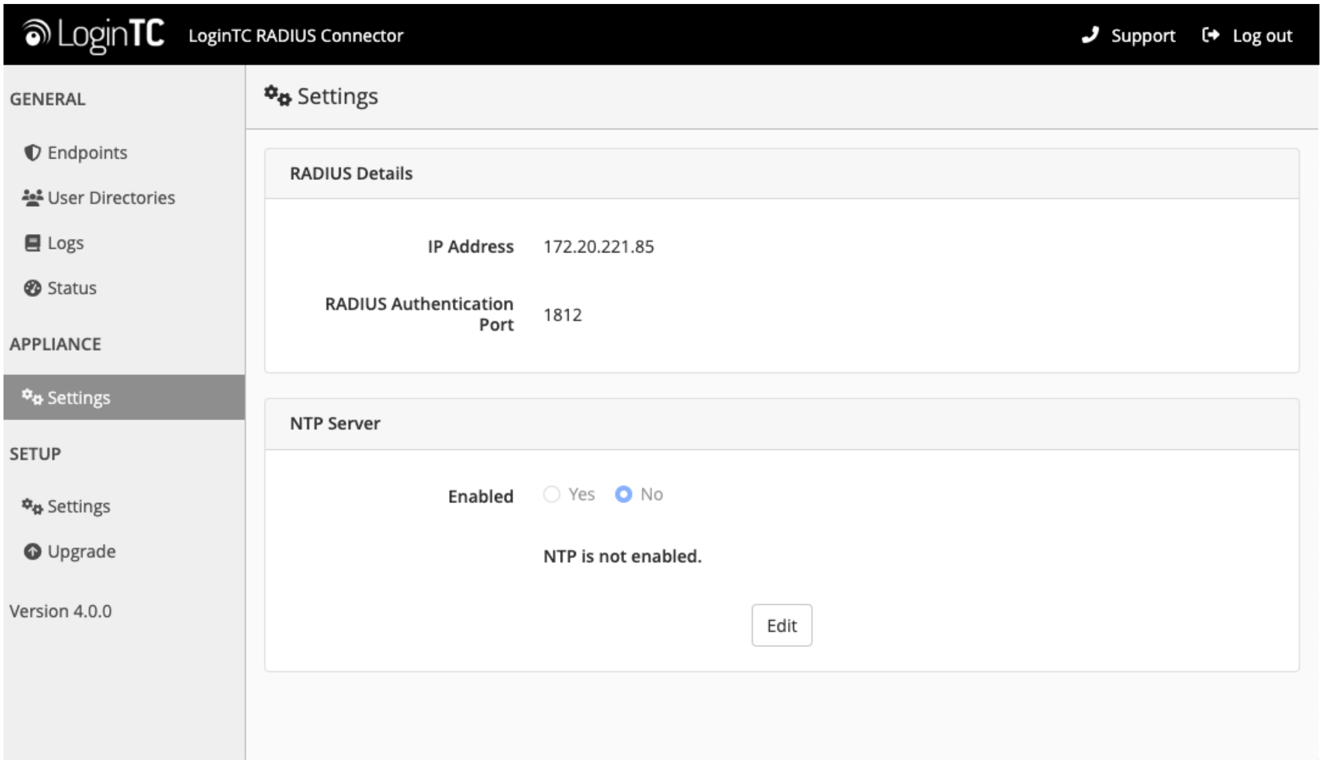
If there was an error during testing, the following will appear:

In this case, click **See logs** (or click the **Logs** section):

Citrix NetScaler Configuration

Once you are satisfied with your setup, configure your Citrix NetScaler to use the LoginTC RADIUS Connector.

For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:



RADIUS Details

IP Address 172.20.221.85

RADIUS Authentication Port 1812

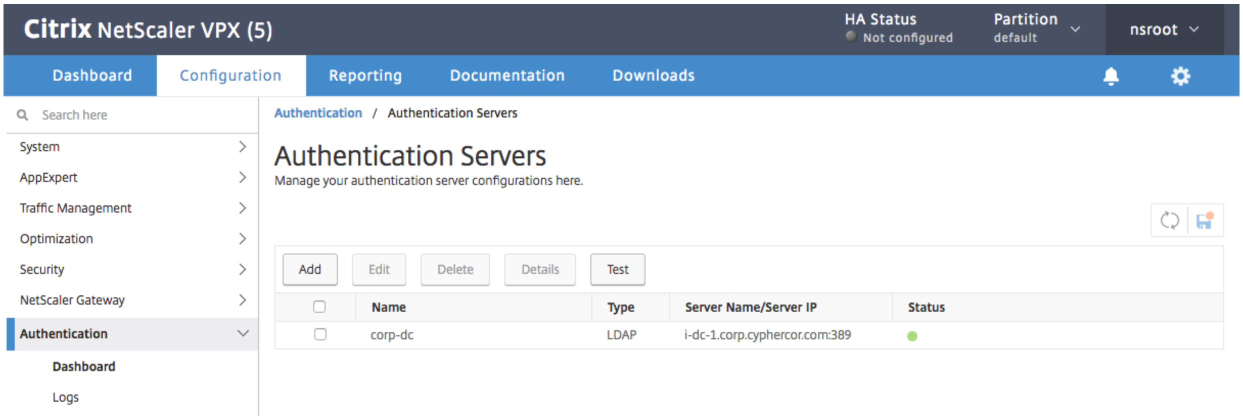
NTP Server

Enabled ○ Yes ● No

NTP is not enabled.

The following are quick steps to set up Citrix NetScaler with LoginTC.

1. Log into the Citrix NetScaler admin web panel
2. Navigate to **Authentication** > **Dashboard**:



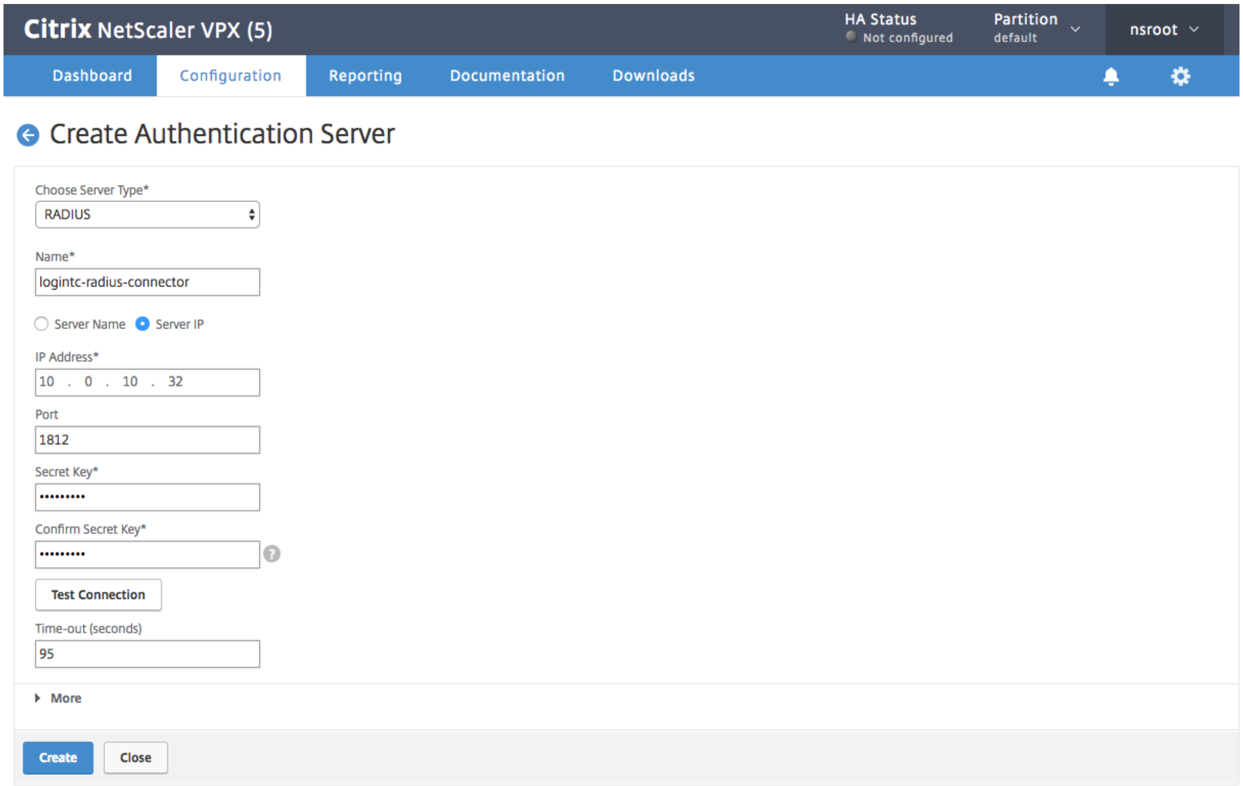
Authentication Servers

Manage your authentication server configurations here.

□	Name	Type	Server Name/Server IP	Status
□	corp-dc	LDAP	i-dc-1.corp.cyphercor.com:389	●

3. Press the add button:

4. Fill in the table



Create Authentication Server

Choose Server Type* RADIUS

Name* logintc-radius-connector

○ Server Name ● Server IP

IP Address* 10 . 0 . 10 . 32

Port 1812

Secret Key* •••••••••

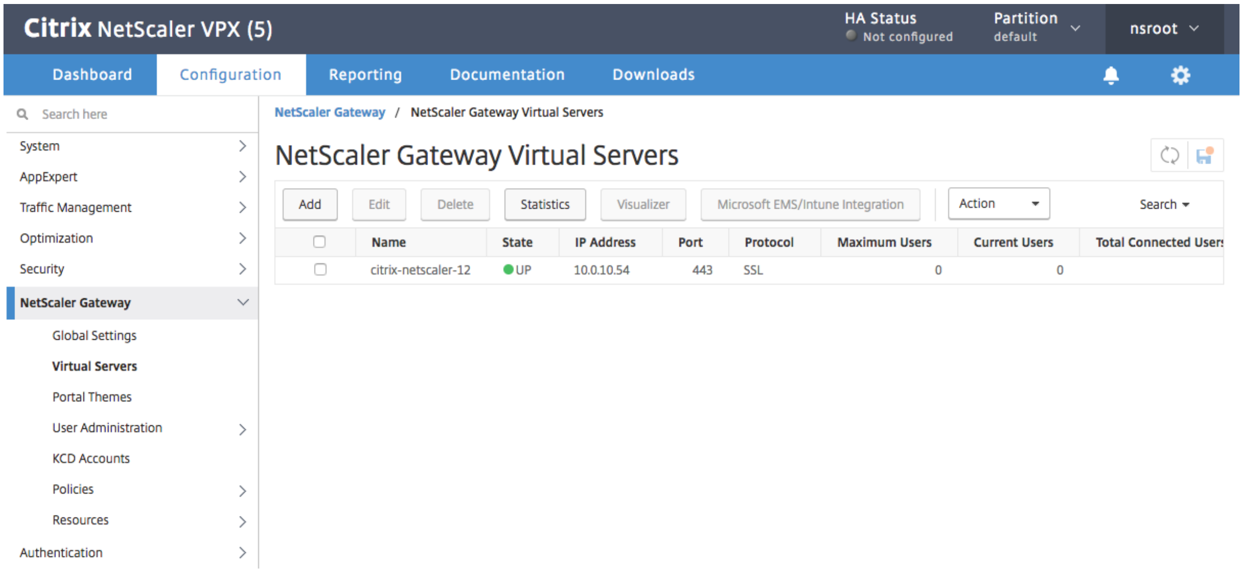
Confirm Secret Key* •••••••••

Time-out (seconds) 95

Property	Description
`Choose Server Type`	Select **RADIUS**
`Name`	Choose a name for this authentication server
`Server Name/IP`	Enter the LoginTC RADIUS Connector FQDN or IP address
`Port`	Enter `1812`
`Server Key`	Enter the RADIUS client secret that you chose on the LoginTC RADIUS Connector
`Confirm Secret Key`	Confirm the secret
`Time-out`	Enter `95`

5. Press **Create**

6. Navigate to **NetScaler Gateway** > **Virtual Servers**

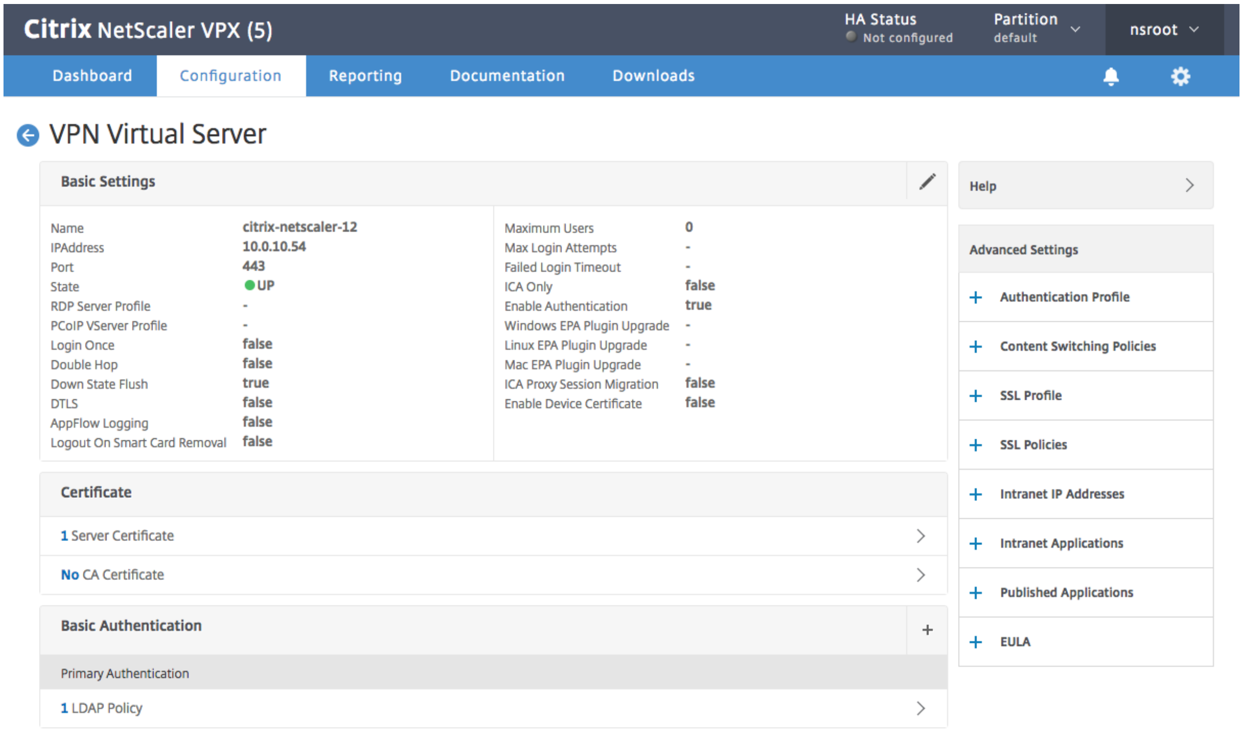


NetScaler Gateway Virtual Servers

☐	Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
☐	citrix-netscaler-12	● UP	10.0.10.54	443	SSL	0	0	

7. Select your virtual server and press **Edit**

8. Press the **+** button in the **Basic Authentication** section:



VPN Virtual Server

Basic Settings

Name	citrix-netscaler-12	Maximum Users	0
IPAddress	10.0.10.54	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	● UP	ICA Only	false
RDP Server Profile	-	Enable Authentication	true
PCoIP VServer Profile	-	Windows EPA Plugin Upgrade	-
Login Once	false	Linux EPA Plugin Upgrade	-
Double Hop	false	Mac EPA Plugin Upgrade	-
Down State Flush	true	ICA Proxy Session Migration	false
DTLS	false	Enable Device Certificate	false
AppFlow Logging	false		
Logout On Smart Card Removal	false		

Certificate

1 Server Certificate

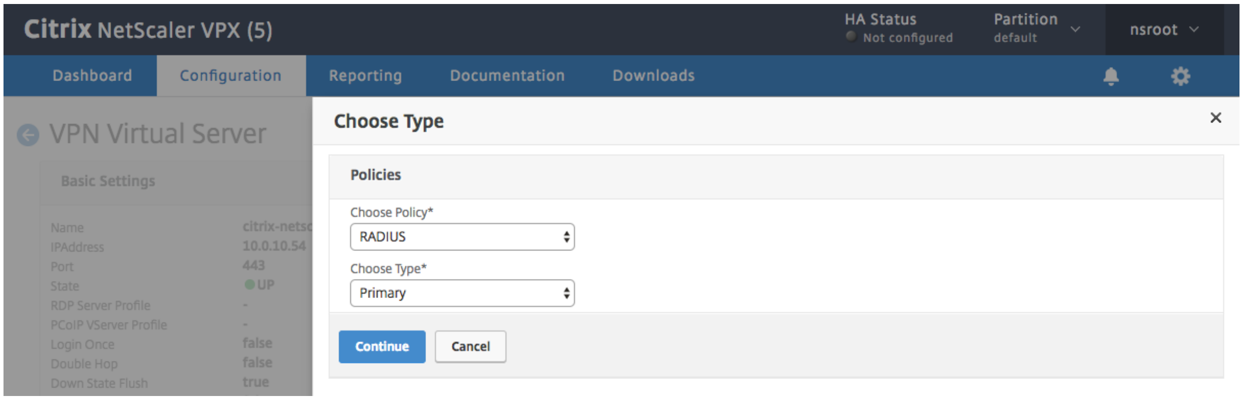
No CA Certificate

Basic Authentication +

Primary Authentication

1 LDAP Policy

9. Select **Primary** as the type:



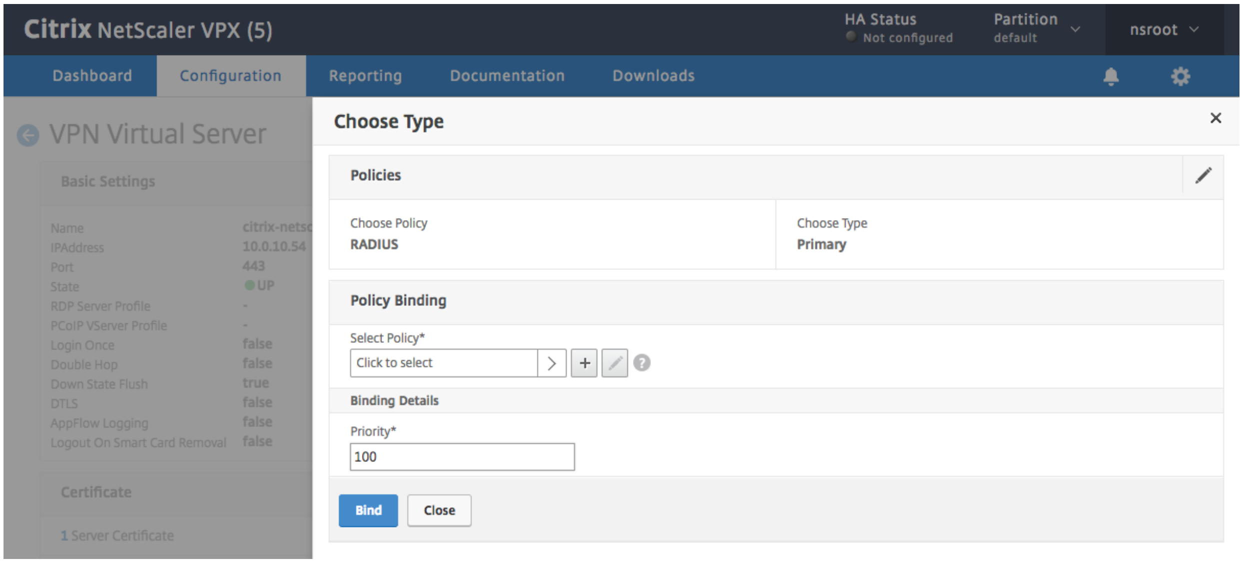
Choose Type

Policies

Choose Policy*: RADIUS

Choose Type*: Primary

10. Press **Continue**
11. Press the **+** button in the **Policy Binding** section or select an existing policy:



Choose Type

Policies

Choose Policy: RADIUS

Choose Type: Primary

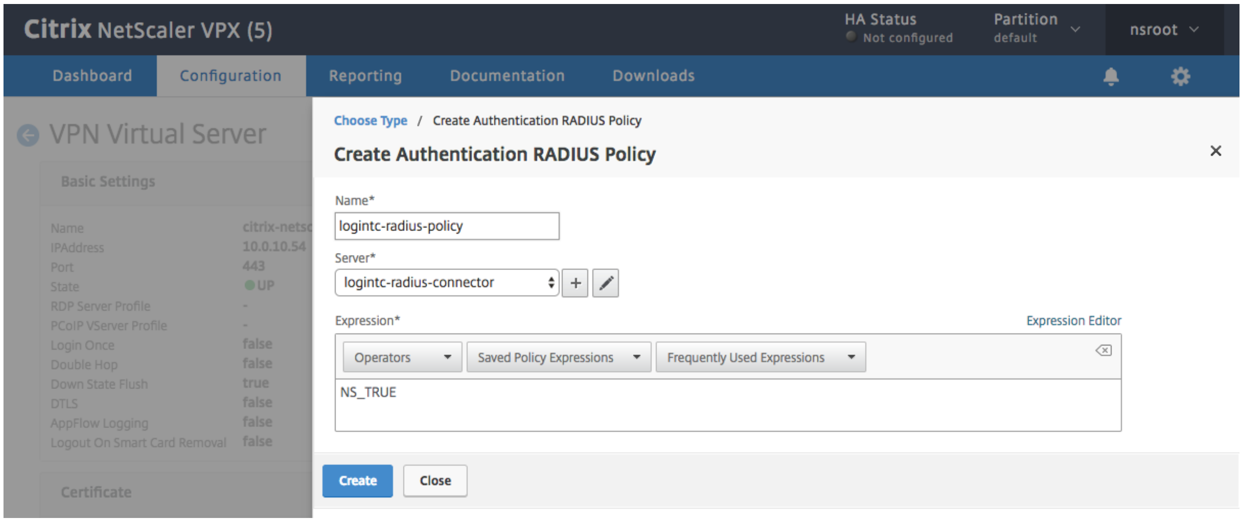
Policy Binding

Select Policy*: Click to select

Binding Details

Priority*: 100

12. Configure your policy for the RADIUS server. Note that you may have to adjust your existing authentication policy so a user or group of users can only authenticate with RADIUS



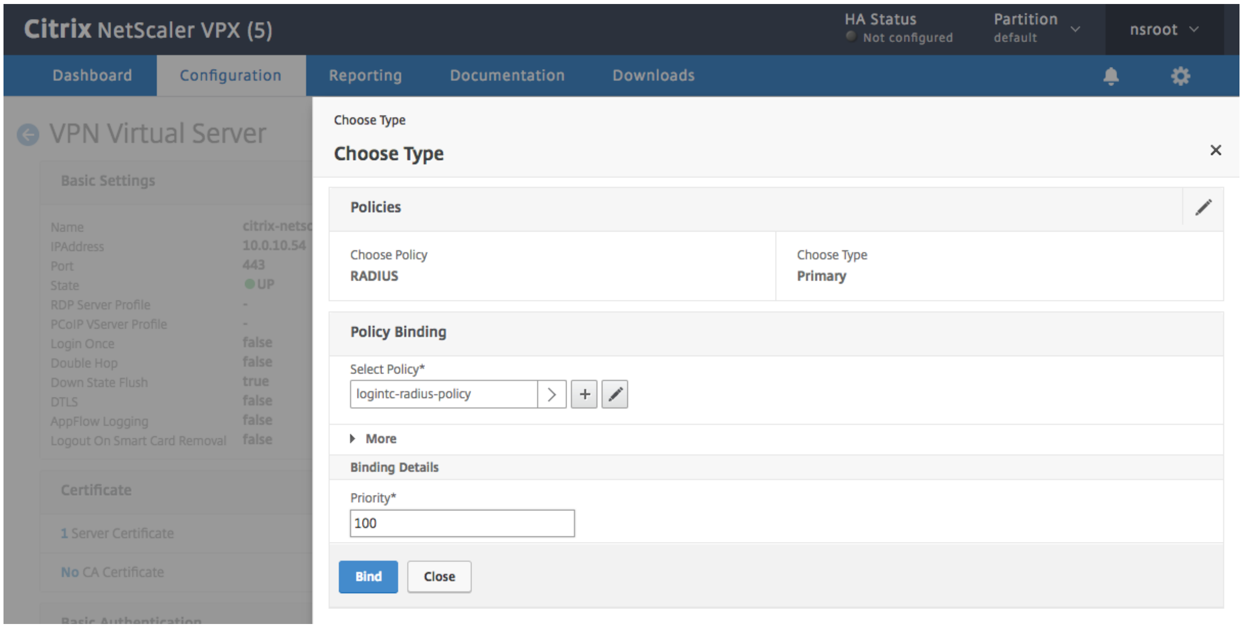
Create Authentication RADIUS Policy

Name*: logintc-radius-policy

Server*: logintc-radius-connector

Expression*: NS_TRUE

13. Press **Done**
14. Press **Bind**:



Name citrix-netsc
IPAddress 10.0.10.54
Port 443
State UP
RDP Server Profile -
PCoIP VServer Profile -
Login Once false
Double Hop false
Down State Flush true
DTLS false
AppFlow Logging false
Logout On Smart Card Removal false

Choose Policy: RADIUS
Choose Type: Primary

Select Policy*: logintc-radius-policy

Priority*: 100

Next configure Citrix to inject the LoginTC Citrix integration snippet for logons. The approach depends on the Citrix version.

Version NS 13.0.88.14 and higher – Addressable AAA Virtual Server

Configure a Rewrite Policy. Create a Rewrite Policy that will insert the LoginTC HTML iframe element.

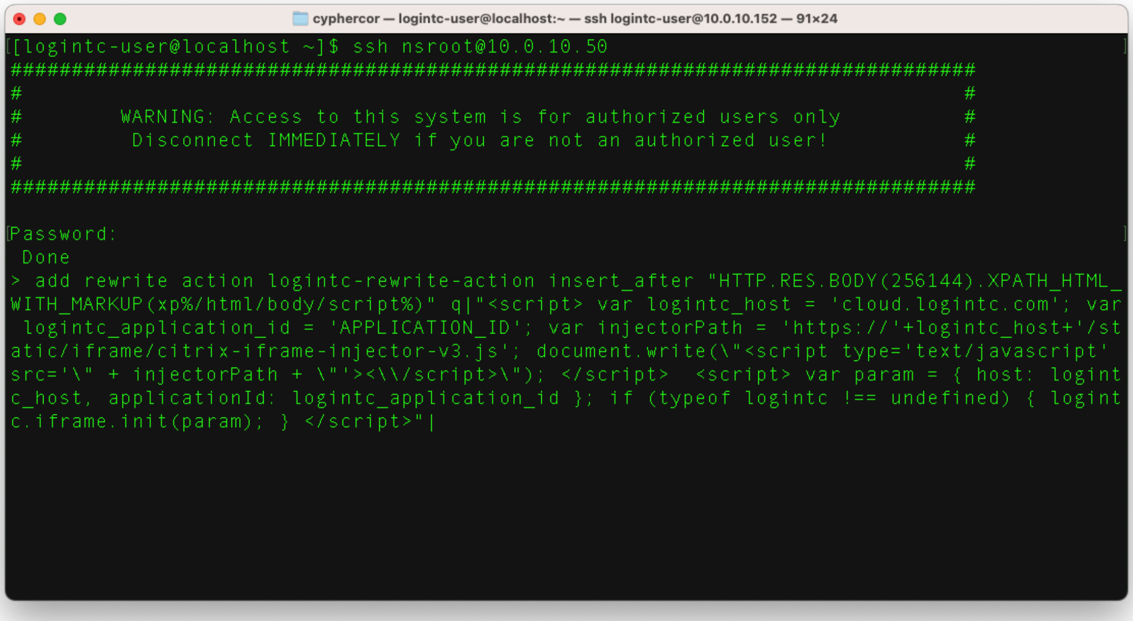
First create a **Rewrite Action** from the command line:

1. Connect to your Citrix NetScaler over SSH:

2. Run command:

```
add rewrite action logintc-rewrite-action insert_after
"HTTP.RES.BODY(256144).XPATH_HTML_WITH_MARKUP(xp%/html/body/script%)" q|"
<script> var logintc_host = 'cloud.logintc.com'; var logintc_application_id =
'APPLICATION_ID'; var injectorPath =
'https://'+logintc_host+'/static/iframe/citrix-iframe-injector-v3.js';
document.write(\"<script type='text/javascript' src='\" + injectorPath + \"'>
<\\/script>\"); </script>  <script> var param = { host: logintc_host,
applicationId: logintc_application_id }; if (typeof logintc !== undefined) {
logintc.iframe.init(param); } </script>"|
```

NOTE: Replace `APPLICATION_ID` with your LoginTC Application ID.



cyphercor — logintc-user@localhost:~ — ssh logintc-user@10.0.10.152 — 91×24

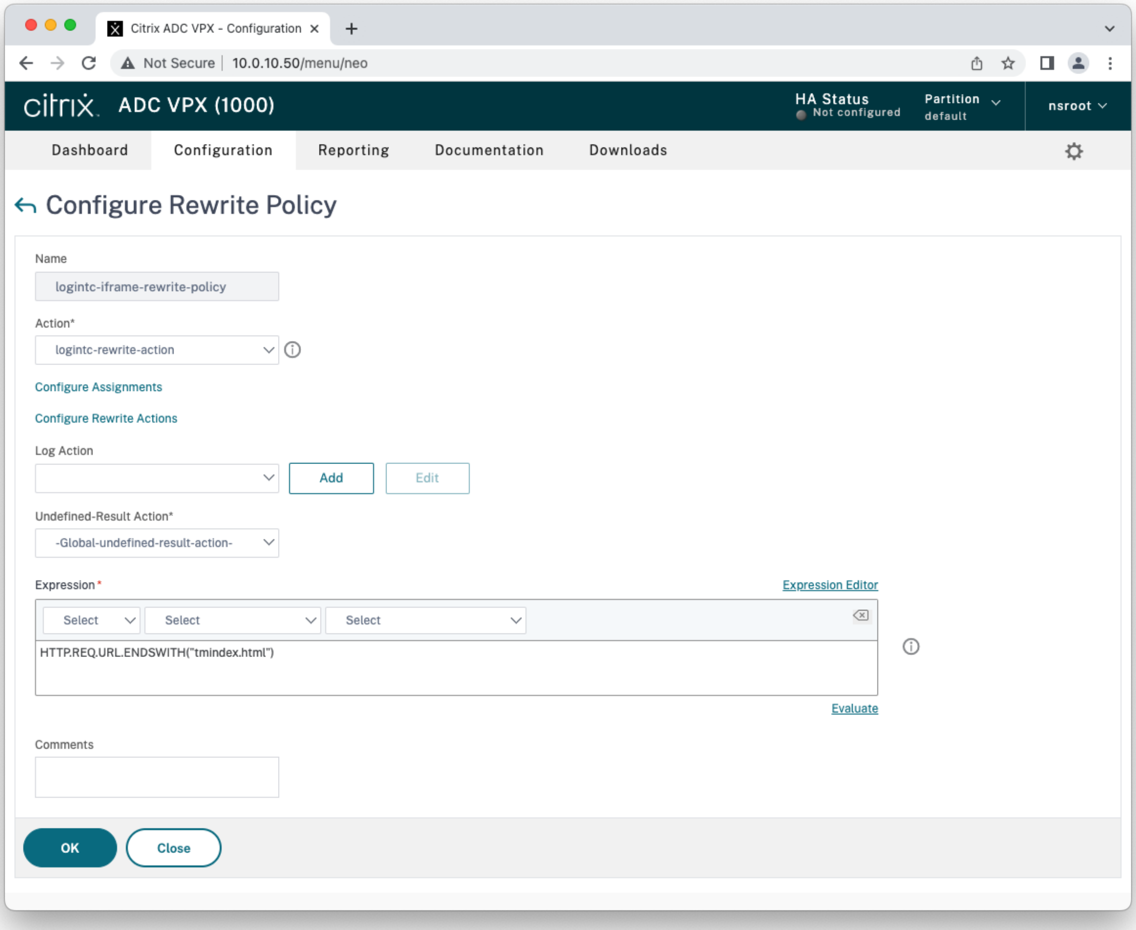
```
[logintc-user@localhost ~]$ ssh nsroot@10.0.10.50
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Password:
 Done
> add rewrite action logintc-rewrite-action insert_after "HTTP.RES.BODY(256144).XPATH_HTML_
WITH_MARKUP(xp%/html/body/script%)" q|"<script> var logintc_host = 'cloud.logintc.com'; var
 logintc_application_id = 'APPLICATION_ID'; var injectorPath = 'https://'+logintc_host+'/st
atic/iframe/citrix-iframe-injector-v3.js'; document.write(\"<script type='text/javascript'
src='\" + injectorPath + \"'><\\/script>\"); </script>  <script> var param = { host: logint
c_host, applicationId: logintc_application_id }; if (typeof logintc !== undefined) { logint
c.iframe.init(param); } </script>"|
```

Create a **Rewrite Policy** from the web GUI:

1. Navigate to **AppExpert** → **Rewrite** → **Policies**
2. Press the **Add** button
3. Set a Name (e.g., “logintc-iframe-rewrite-policy”)
4. In the **Action** drop down select the newly created Rewrite Action (e.g. “logintc-rewrite-action”)
5. Enter **Expression**:

```
HTTP.REQ.URL.ENDSWITH("/logon/LogonPoint/tmindex.html")
```

6. Click **OK** to save the Create the Rewrite Policy



Configure Rewrite Policy

Name: logintc-iframe-rewrite-policy

Action*: logintc-rewrite-action

Log Action:

Undefined-Result Action*: -Global-undefined-result-action-

Expression*:

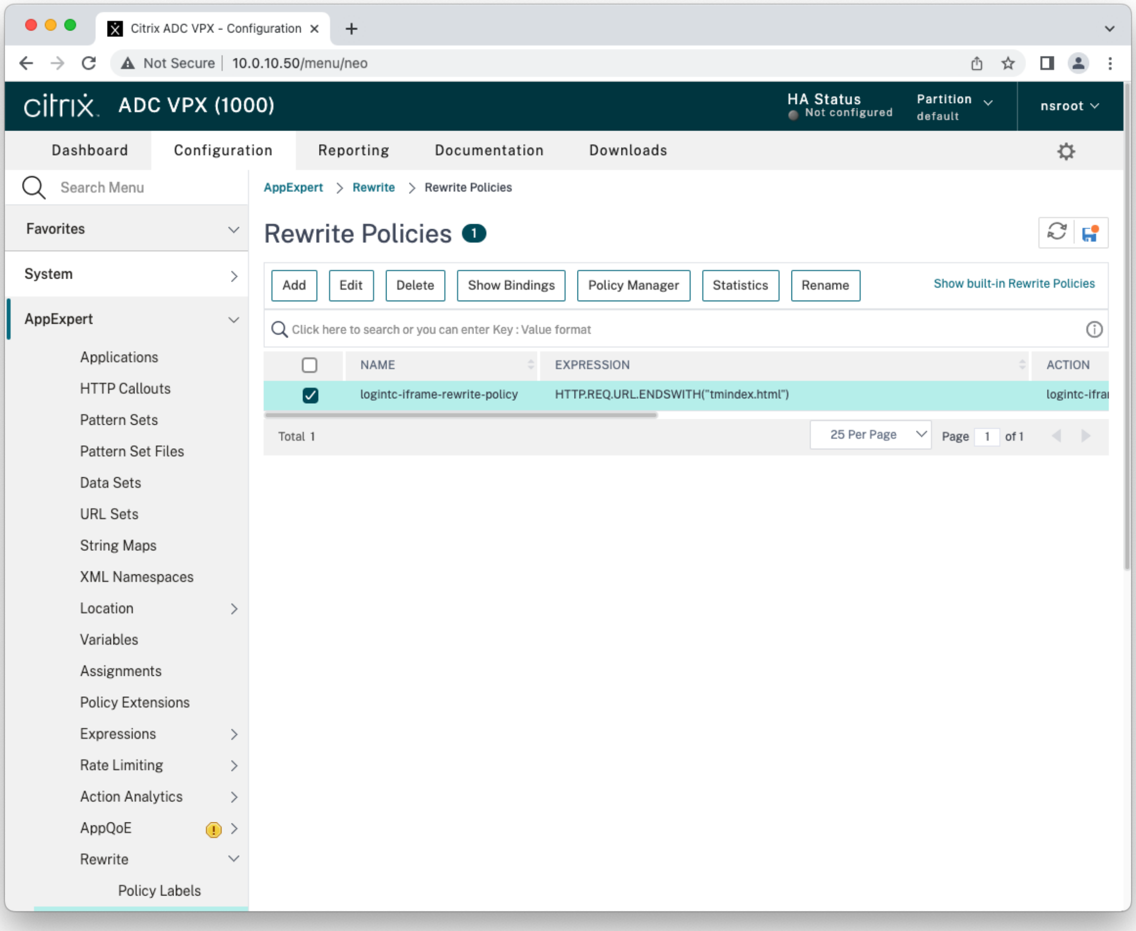
```
HTTP.REQ.URL.ENDSWITH("tmindex.html")
```

Comments:

Now bind this newly created **Rewrite Policy** as a global policy:

1. Navigate to **AppExpert** → **Rewrite** → **Rewrite Policies**

2. Select the newly created rewrite policy

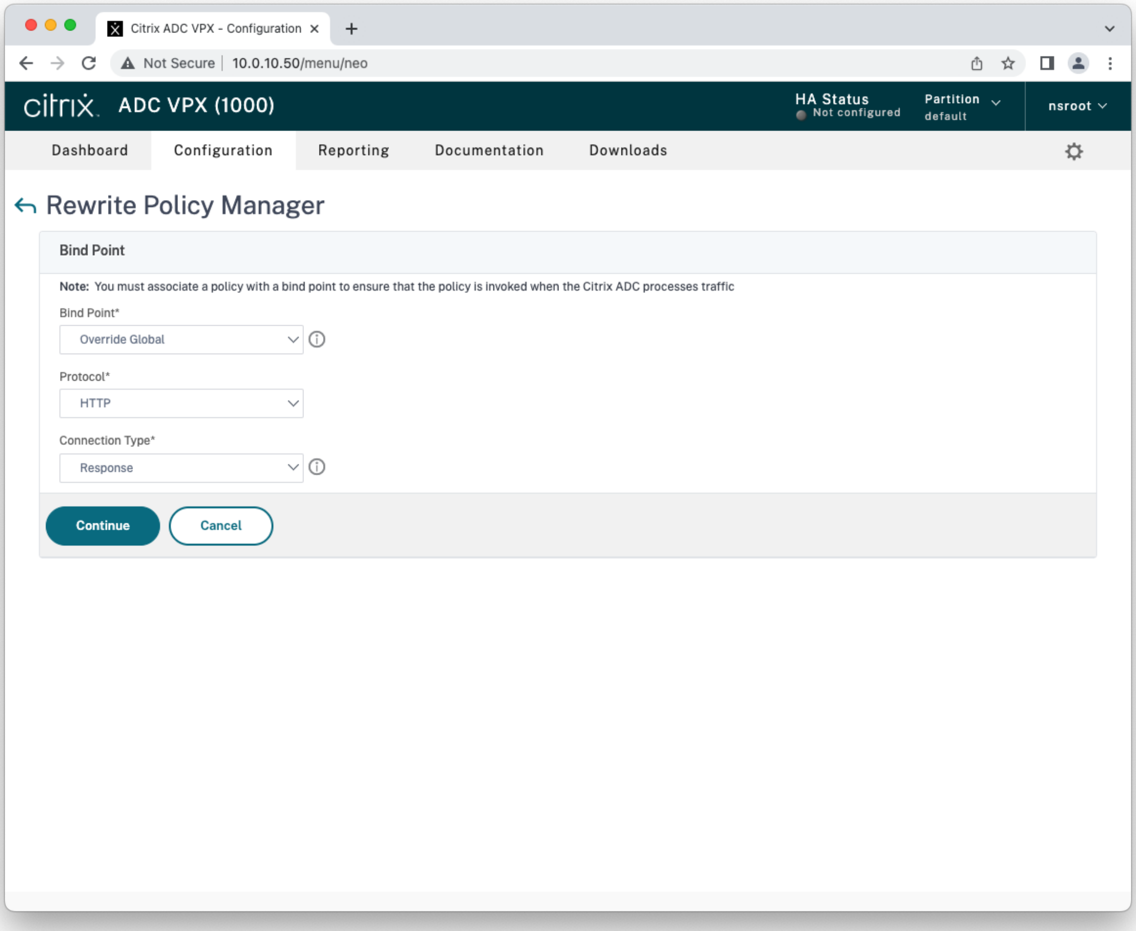


□	NAME	EXPRESSION	ACTION
☑	logintc-iframe-rewrite-policy	HTTP.REQ.URL.ENDSWITH("tmindex.html")	logintc-ifra

Total 1 | 25 Per Page | Page 1 of 1

3. Press the **Policy Manager** button
4. Set **Bind Point** to Override Global
5. Set **Protocol** to HTTP
6. Set **Connection Type** to Response

7. Press the **Continue** button



Rewrite Policy Manager

Bind Point

Note: You must associate a policy with a bind point to ensure that the policy is invoked when the Citrix ADC processes traffic

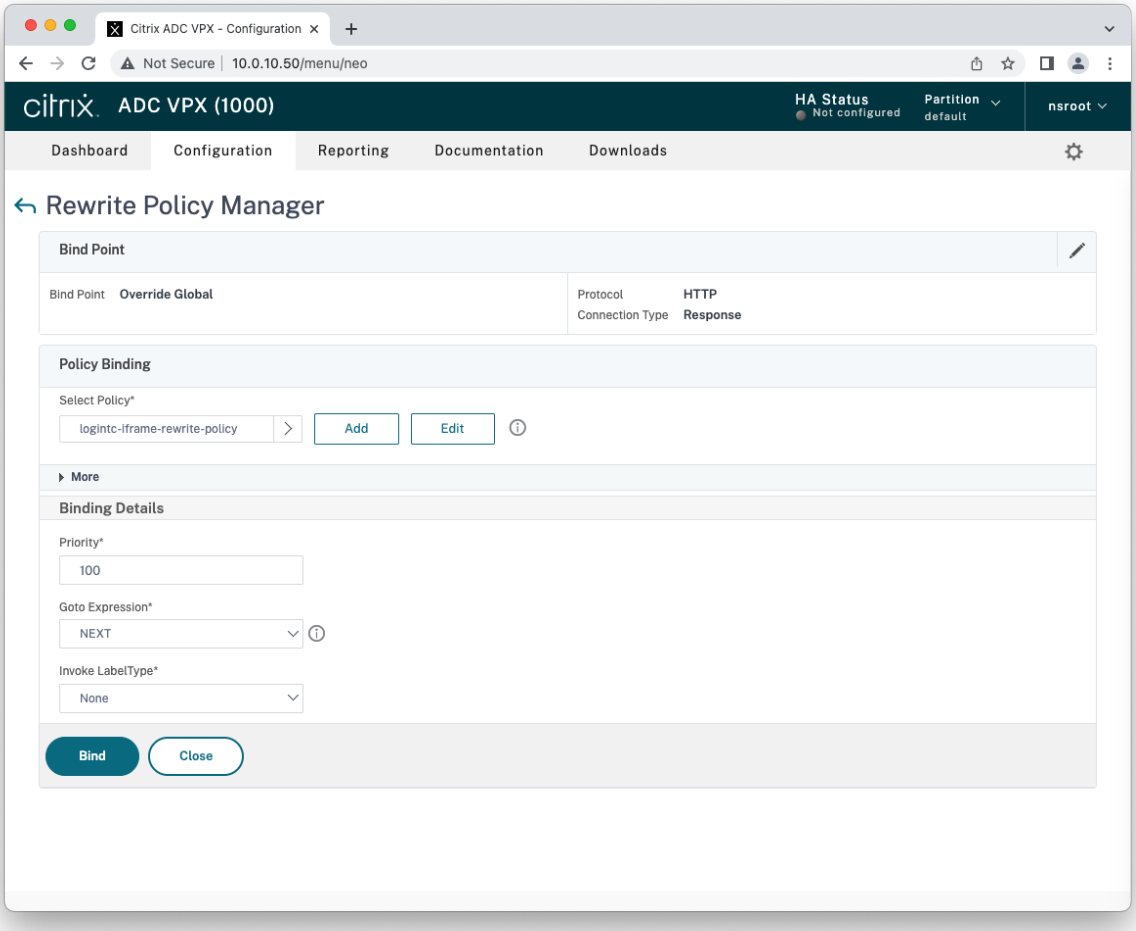
Bind Point*: Override Global

Protocol*: HTTP

Connection Type*: Response

8. Click on the arrow under **Select Policy** and select the newly created policy (e.g, “logintc-iframe-rewrite-policy”)
9. Set **Goto Expression** to NEXT

10. Press the **Bind** button



Rewrite Policy Manager

Bind Point

Bind Point Override Global

Protocol HTTP

Connection Type Response

Policy Binding

Select Policy* logintc-iframe-rewrite-policy

Binding Details

Priority* 100

Goto Expression* NEXT

Invoke LabelType* None

Version NS 13.0.88.14 and higher – Non-Addressable AAA Virtual Server

Configure a Rewrite Policy. Create a Rewrite Policy that will insert the LoginTC HTML iframe element.

First create a **Rewrite Action** from the command line:

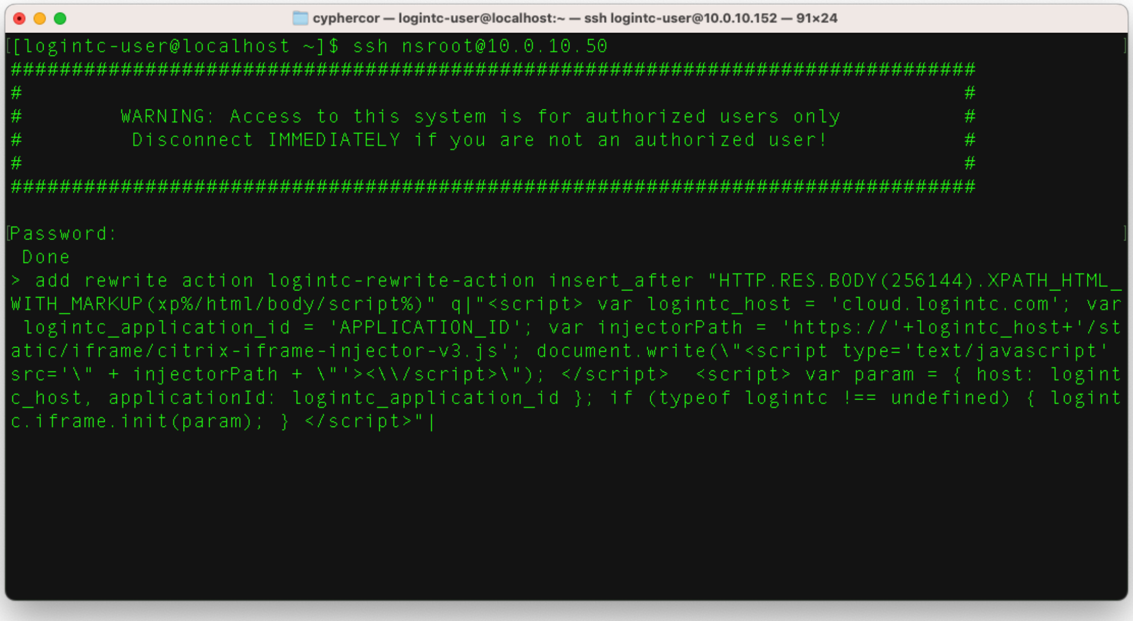
First create a **Rewrite Action** from the command line:

1. Connect to your Citrix NetScaler over SSH:

2. Run command:

```
add rewrite action logintc-rewrite-action insert_after
"HTTP.RES.BODY(256144).XPATH_HTML_WITH_MARKUP(xp%/html/body/script%)" q|"
<script> var logintc_host = 'cloud.logintc.com'; var logintc_application_id =
'APPLICATION_ID'; var injectorPath =
'https://'+logintc_host+'/static/iframe/citrix-iframe-injector-v3.js';
document.write(\"<script type='text/javascript' src='\" + injectorPath + \"'>
<\\/script>\"); </script>  <script> var param = { host: logintc_host,
applicationId: logintc_application_id }; if (typeof logintc !== undefined) {
logintc.iframe.init(param); } </script>"|
```

NOTE: Replace `APPLICATION_ID` with your LoginTC Application ID.


cyphercor — logintc-user@localhost:~ — ssh logintc-user@10.0.10.152 — 91×24

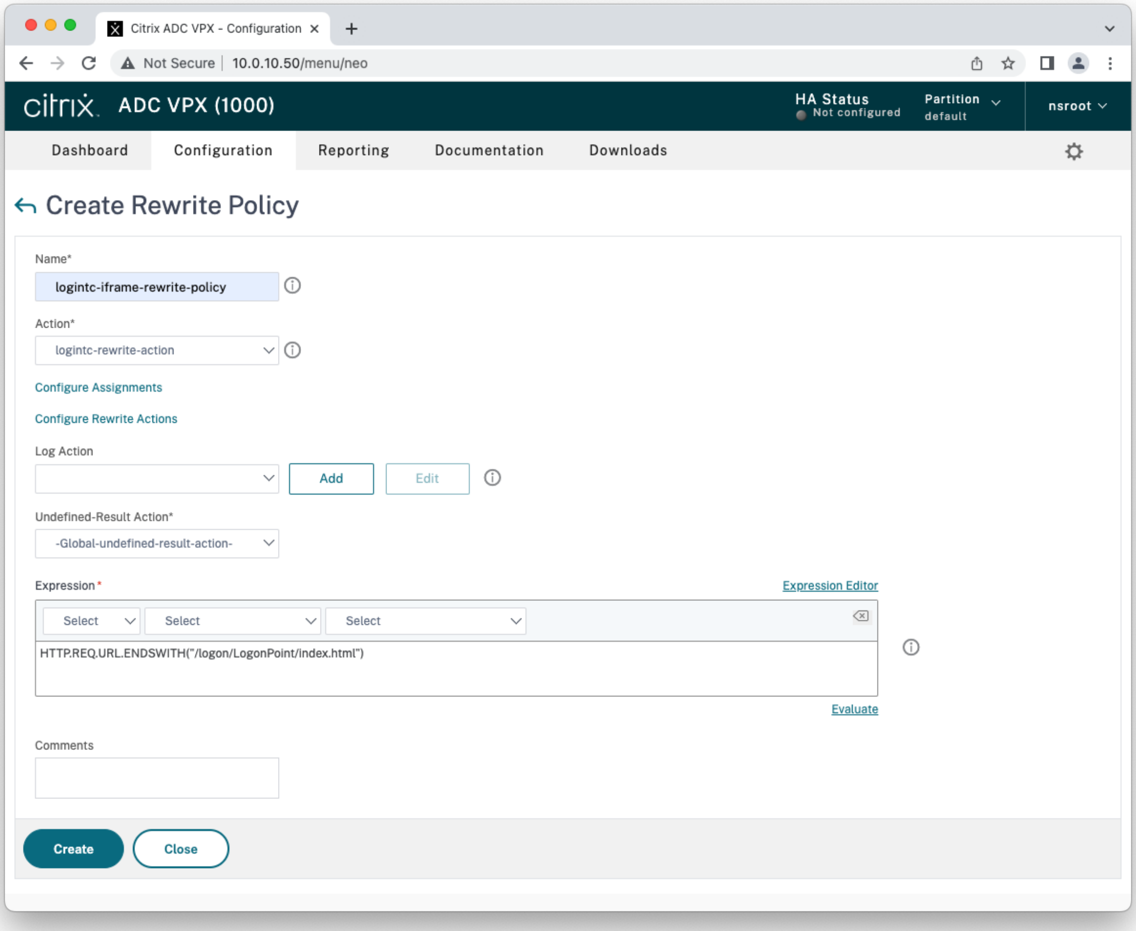
```
[logintc-user@localhost ~]$ ssh nsroot@10.0.10.50
###############################################################################
#                                                                             #
#        WARNING: Access to this system is for authorized users only          #
#         Disconnect IMMEDIATELY if you are not an authorized user!           #
#                                                                             #
###############################################################################

Password:
 Done
> add rewrite action logintc-rewrite-action insert_after "HTTP.RES.BODY(256144).XPATH_HTML_
WITH_MARKUP(xp%/html/body/script%)" q|"<script> var logintc_host = 'cloud.logintc.com'; var
 logintc_application_id = 'APPLICATION_ID'; var injectorPath = 'https://'+logintc_host+'/st
atic/iframe/citrix-iframe-injector-v3.js'; document.write(\"<script type='text/javascript'
src='\" + injectorPath + \"'><\\/script>\"); </script>  <script> var param = { host: logint
c_host, applicationId: logintc_application_id }; if (typeof logintc !== undefined) { logint
c.iframe.init(param); } </script>"|
```

Create a **Rewrite Policy** from the web GUI:

1. Navigate to **AppExpert** → **Rewrite** → **Policies**
2. Press the **Add** button
3. Set a Name (e.g., “logintc-iframe-rewrite-policy”)
4. In the **Action** drop down select the newly created Rewrite Action (e.g. “logintc-rewrite-action”)
5. Enter **Expression**:

```
HTTP.REQ.URL.ENDSWITH("/logon/LogonPoint/index.html")
```

6. Click **OK** to save the Create the Rewrite Policy



Create Rewrite Policy

Name*: logintc-iframe-rewrite-policy

Action*: logintc-rewrite-action

Log Action:

Undefined-Result Action*: -Global-undefined-result-action-

Expression*:

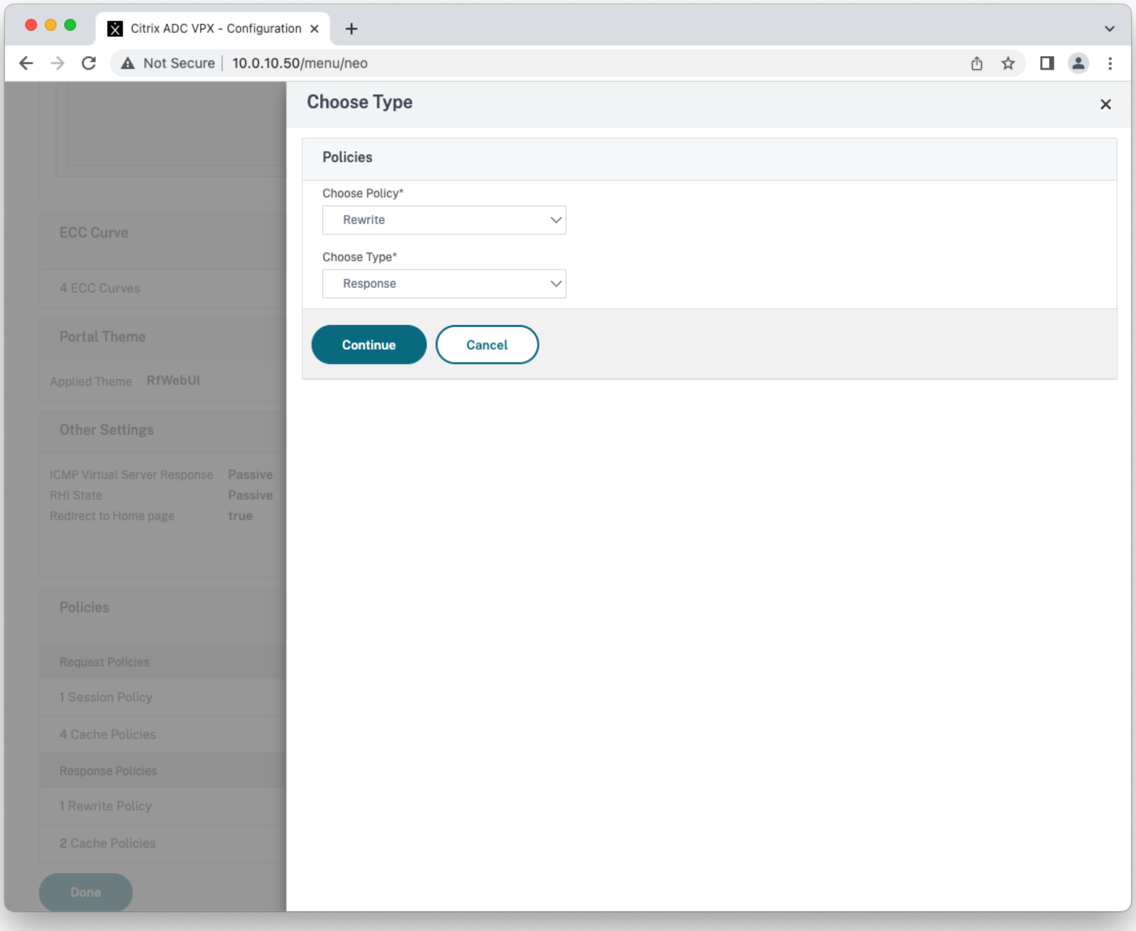
```
HTTP.REQ.URL.ENDSWITH("/logon/LogonPoint/index.html")
```

Comments:

Now bind this newly created **Rewrite Policy** to the NetScaler Gateway virtual server:

1. Navigate to **NetScaler Gateway** → **Virtual Servers**
2. Select the target virtual server and press the **Edit** button to view the virtual server settings page
3. Press the **+ button** in the **Policies** section to add a new policy
4. Set **Choose Policy** to Rewrite
5. Set **Choose Type** to Response

6. Press the **Continue** button



Choose Type

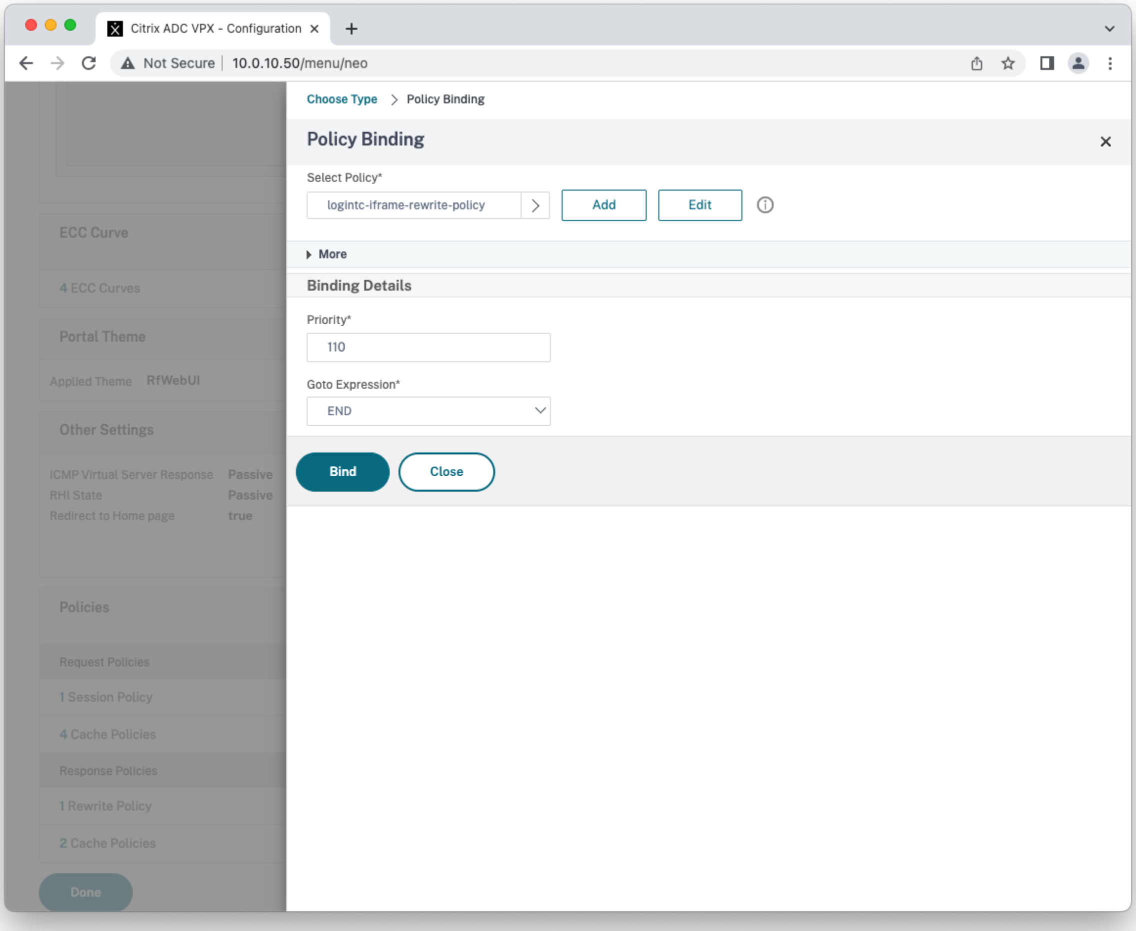
Policies

Choose Policy* Rewrite

Choose Type* Response

7. Click **Add Binding**
8. Click on **"Click to select"** for **Select Policy** to select a rewrite policy
9. Select the LoginTC iframe rewrite policy (e.g., "logintc-iframe-rewrite-policy")
10. Press the **Select** button

11. Press the **Bind** button



Select Policy*: logintc-iframe-rewrite-policy

Priority*: 110

Goto Expression*: END

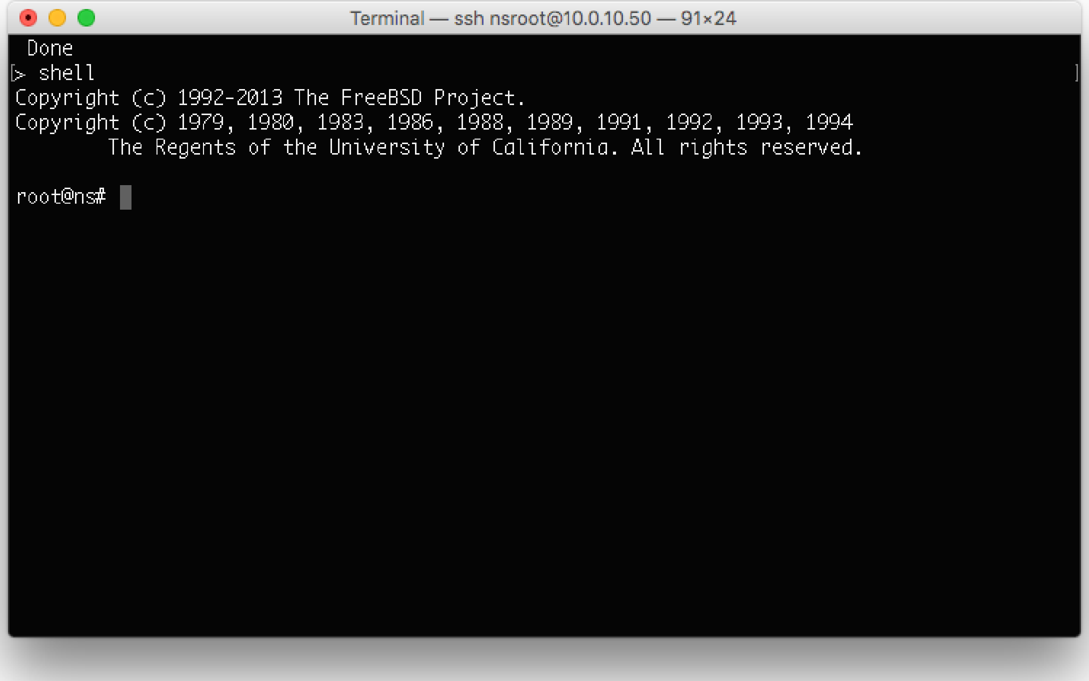
Applied Theme RfWebUI

ICMP Virtual Server Response Passive
RHI State Passive
Redirect to Home page true

Version NS13.0 87.9 and lower

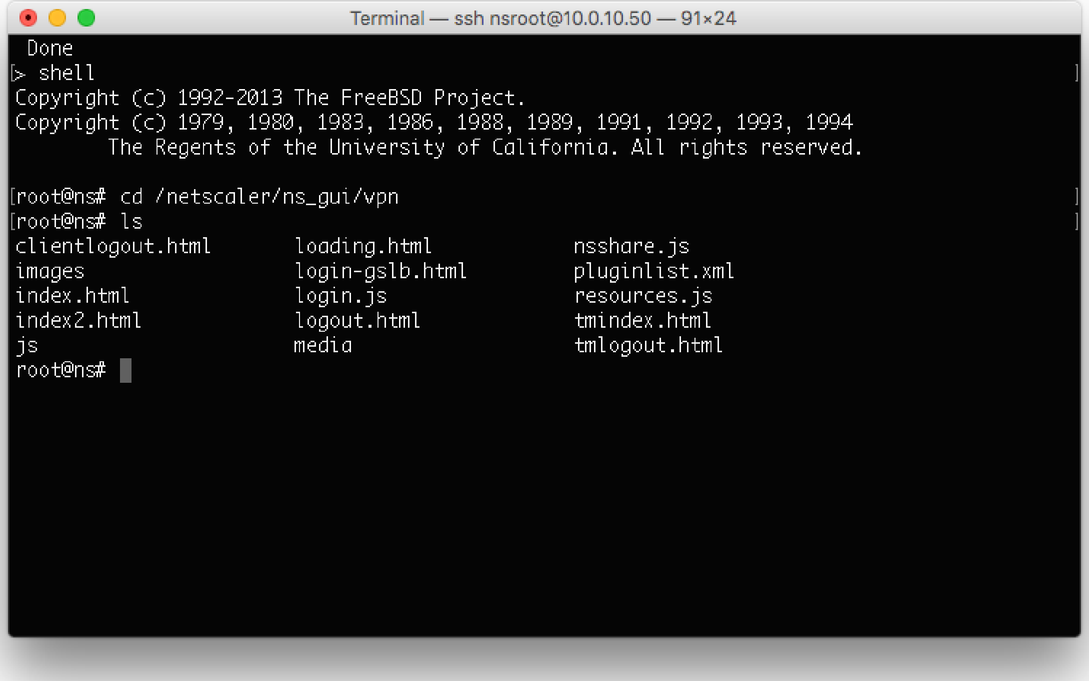
1. Connect to your Citrix NetScaler over SSH:

2. Run command: `shell`



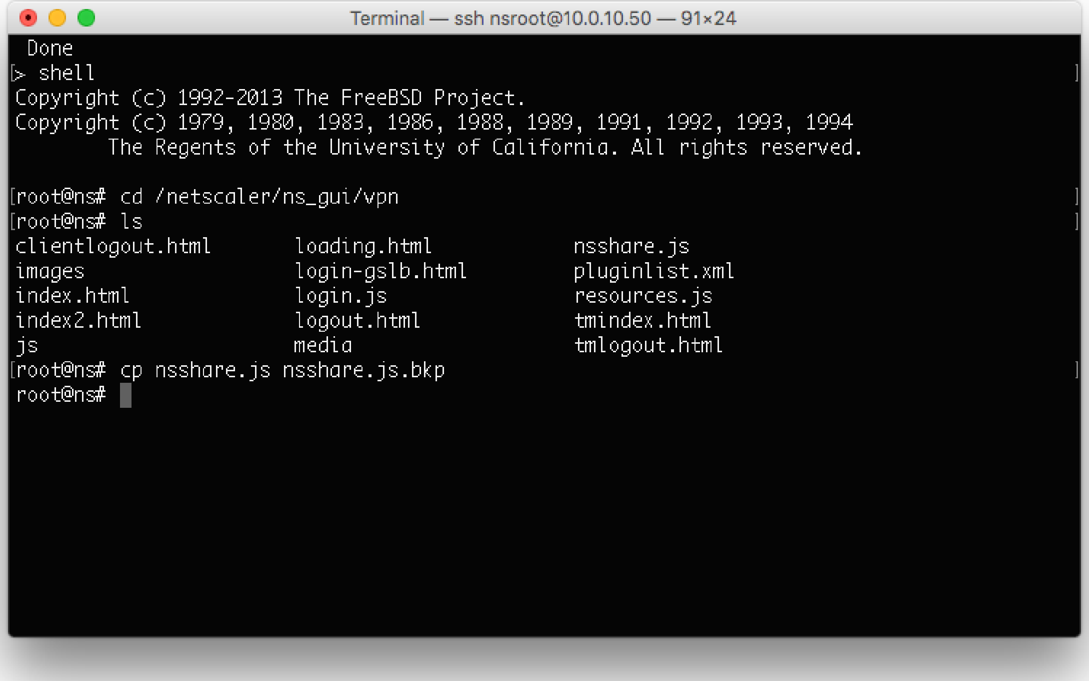
```
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns#
```

3. Run command: `cd /netscaler/ns_gui/vpn`



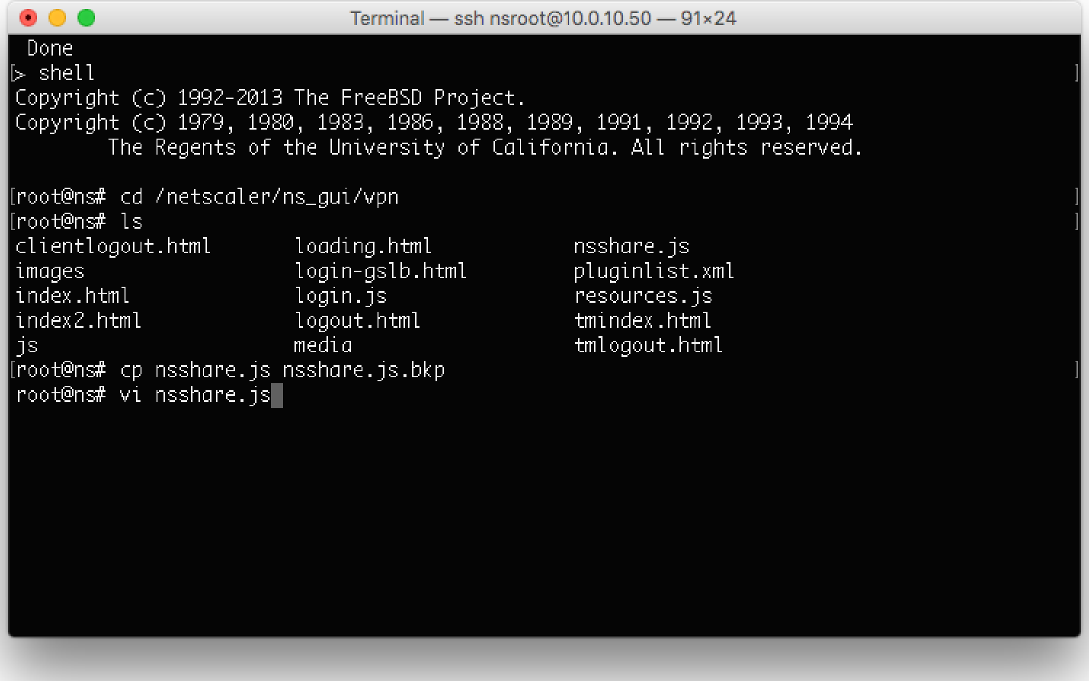
```
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# cd /netscaler/ns_gui/vpn
root@ns# ls
clientlogout.html       loading.html            nsshare.js
images                  login-gslb.html         pluginlist.xml
index.html              login.js                resources.js
index2.html             logout.html             tmindex.html
js                      media                   tmlogout.html
root@ns#
```

4. Create a backup of `nsshare.js` file: `cp nsshare.js nsshare.js.bkp`



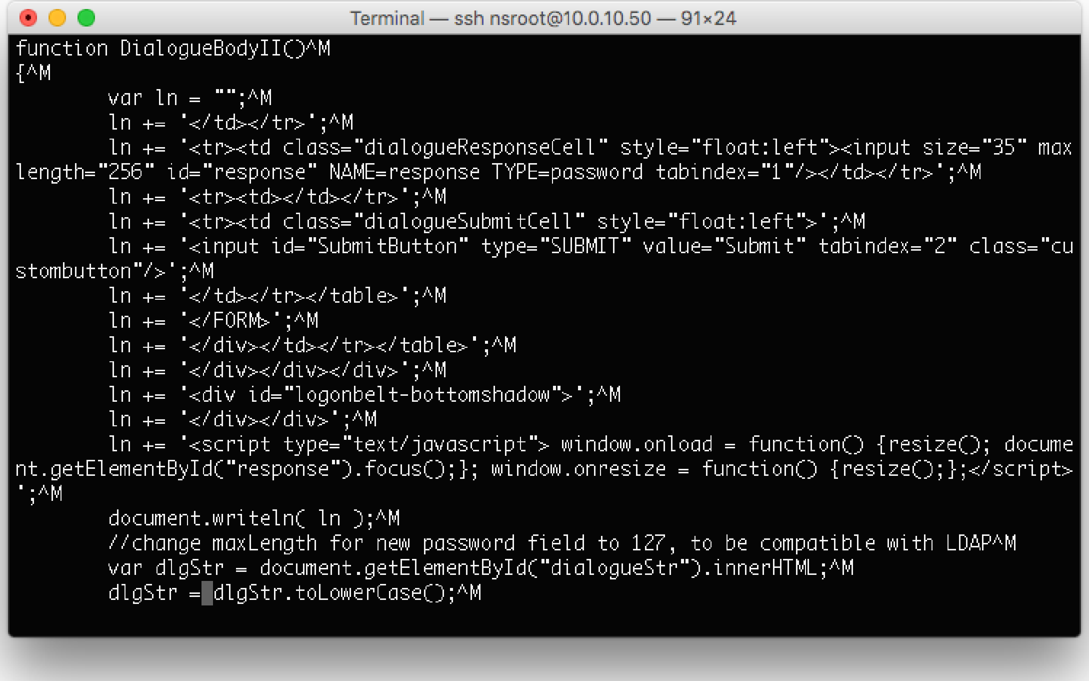
```
 Done
[> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

[root@ns# cd /netscaler/ns_gui/vpn
[root@ns# ls
clientlogout.html       loading.html            nsshare.js
images                  login-gslb.html         pluginlist.xml
index.html              login.js                resources.js
index2.html             logout.html             tmindex.html
js                      media                   tmlogout.html
[root@ns# cp nsshare.js nsshare.js.bkp
root@ns# 
```

5. Open file `nsshare.js` for editing: `vi nsshare.js`



```
 Done
[> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

[root@ns# cd /netscaler/ns_gui/vpn
[root@ns# ls
clientlogout.html       loading.html            nsshare.js
images                  login-gslb.html         pluginlist.xml
index.html              login.js                resources.js
index2.html             logout.html             tmindex.html
js                      media                   tmlogout.html
[root@ns# cp nsshare.js nsshare.js.bkp
root@ns# vi nsshare.js
```

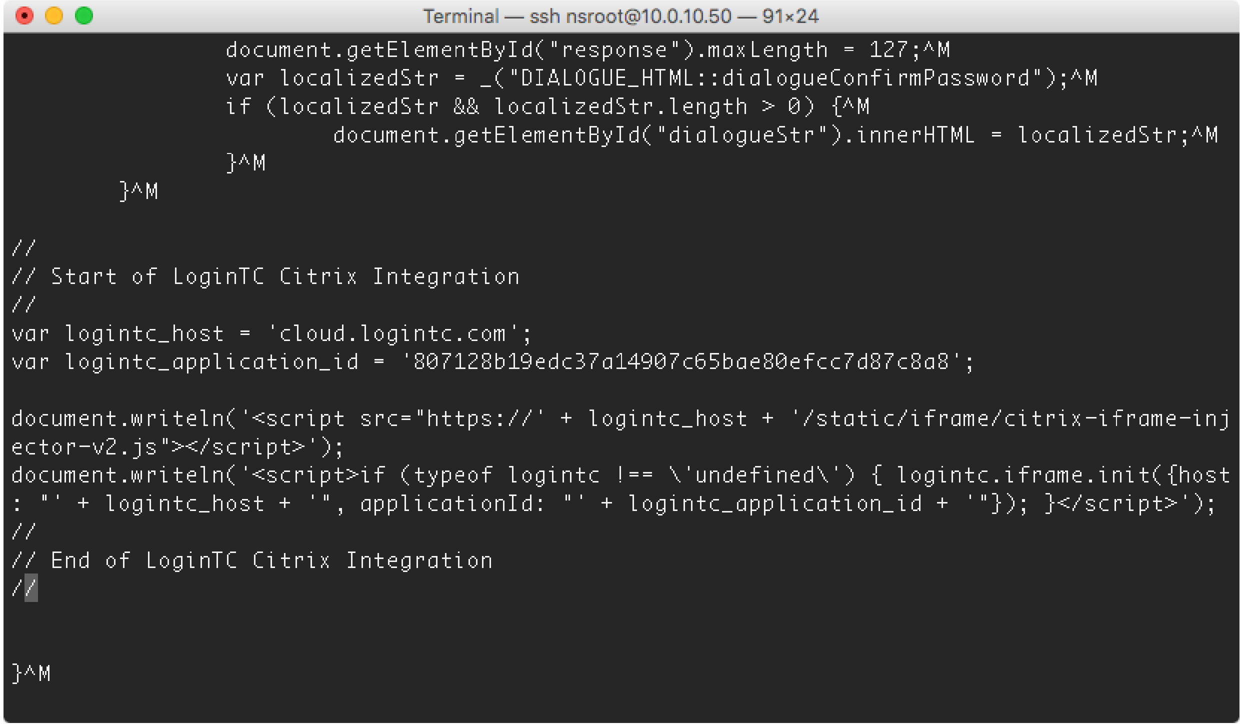
6. Scroll down to the `DialogueBodyII()` function:



```
function DialogueBodyII()^M
{^M
        var ln = "";^M
        ln += '</td></tr>';^M
        ln += '<tr><td class="dialogueResponseCell" style="float:left"><input size="35" max
length="256" id="response" NAME=response TYPE=password tabindex="1"/></td></tr>';^M
        ln += '<tr><td></td></tr>';^M
        ln += '<tr><td class="dialogueSubmitCell" style="float:left">';^M
        ln += '<input id="SubmitButton" type="SUBMIT" value="Submit" tabindex="2" class="cu
stombutton"/>';^M
        ln += '</td></tr></table>';^M
        ln += '</FORM>';^M
        ln += '</div></td></tr></table>';^M
        ln += '</div></div></div>';^M
        ln += '<div id="logonbelt-bottomshadow">';^M
        ln += '</div></div>';^M
        ln += '<script type="text/javascript"> window.onload = function() {resize(); docume
nt.getElementById("response").focus();}; window.onresize = function() {resize();};</script>
';^M
        document.writeln( ln );^M
        //change maxLength for new password field to 127, to be compatible with LDAP^M
        var dlgStr = document.getElementById("dialogueStr").innerHTML;^M
        dlgStr = dlgStr.toLowerCase();^M
```

7. Scroll down to the bottom of the `DialogueBodyII()` function and insert the Citrix Integration snippet (https://www.logintc.com/downloads/citrix-code-snippet-v1-app.txt):

```
            //
            // Start of LoginTC Citrix Integration
            //
            var logintc_host = 'cloud.logintc.com';
            var logintc_application_id = 'YOUR_APPLICATION_ID';
            document.writeln('<script src="https://' + logintc_host +
'/static/iframe/citrix-iframe-injector-v2.js"></script>');
            document.writeln('<script>if (typeof logintc !== \'undefined\') {
logintc.iframe.init({host: "' + logintc_host + '", applicationId: "' +
logintc_application_id + '"}); }</script>');
            //
            // End of LoginTC Citrix Integration
            //
```



Terminal — ssh nsroot@10.0.10.50 — 91×24

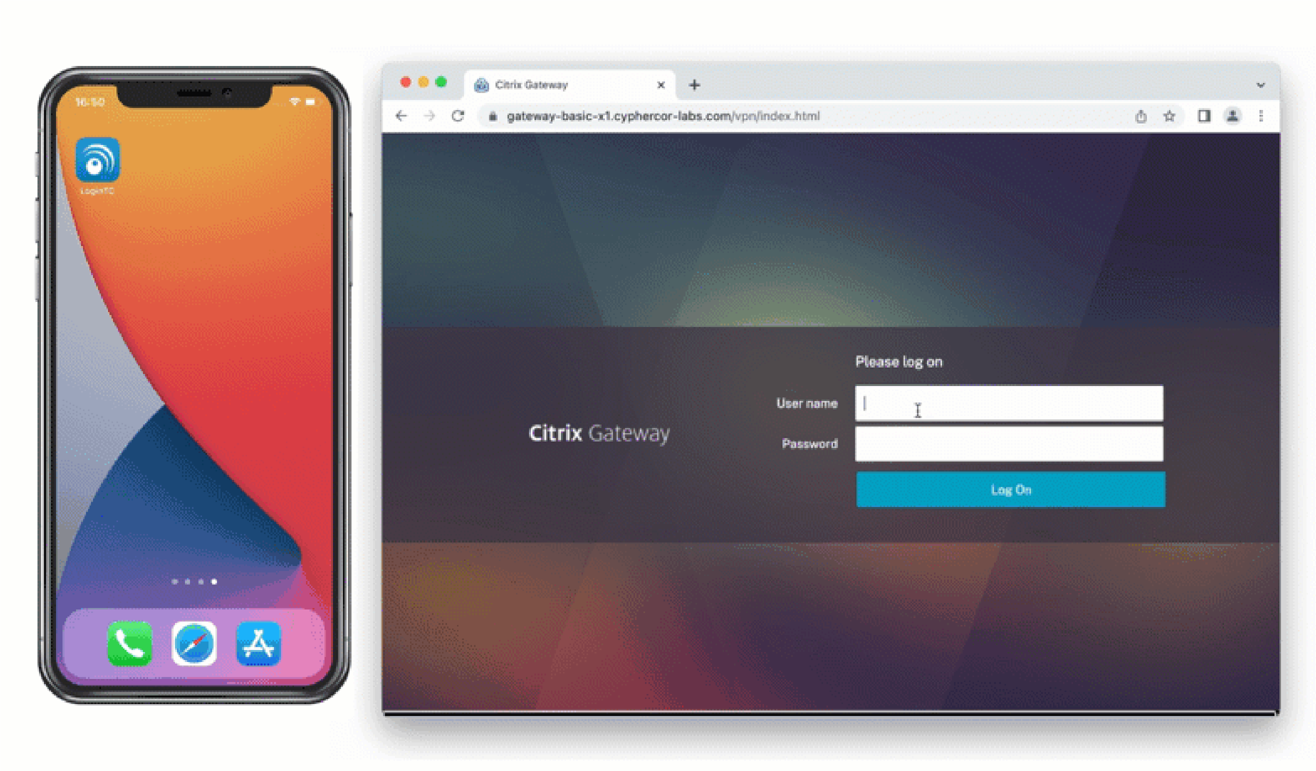
```
                document.getElementById("response").maxLength = 127;^M
                var localizedStr = _("DIALOGUE_HTML::dialogueConfirmPassword");^M
                if (localizedStr && localizedStr.length > 0) {^M
                        document.getElementById("dialogueStr").innerHTML = localizedStr;^M
                }^M
        }^M

//
// Start of LoginTC Citrix Integration
//
var logintc_host = 'cloud.logintc.com';
var logintc_application_id = '807128b19edc37a14907c65bae80efcc7d87c8a8';

document.writeln('<script src="https://' + logintc_host + '/static/iframe/citrix-iframe-inj
ector-v2.js"></script>');
document.writeln('<script>if (typeof logintc !== \'undefined\') { logintc.iframe.init({host
: "' + logintc_host + '", applicationId: "' + logintc_application_id + '"}); }</script>');
//
// End of LoginTC Citrix Integration
//


}^M
```

Ensure that you have entered your `Application ID` in the Citrix Integration snippet, retrieve Application ID

8. To persist these changes between reboots run commands: `cp /netscaler/ns_gui/vpn/nsshare.js /var/vpn/vpn/nsshare.js` and `cp /netscaler/ns_gui/vpn/nsshare.js.bkp /var/vpn/vpn/nsshare.js.bkp`

Your NetScaler is now configured to use the LoginTC RADIUS Connector for authentication.

To test, navigate to the logon page using the access policy just configured and attempt to login. You should be prompted with a LoginTC login form:

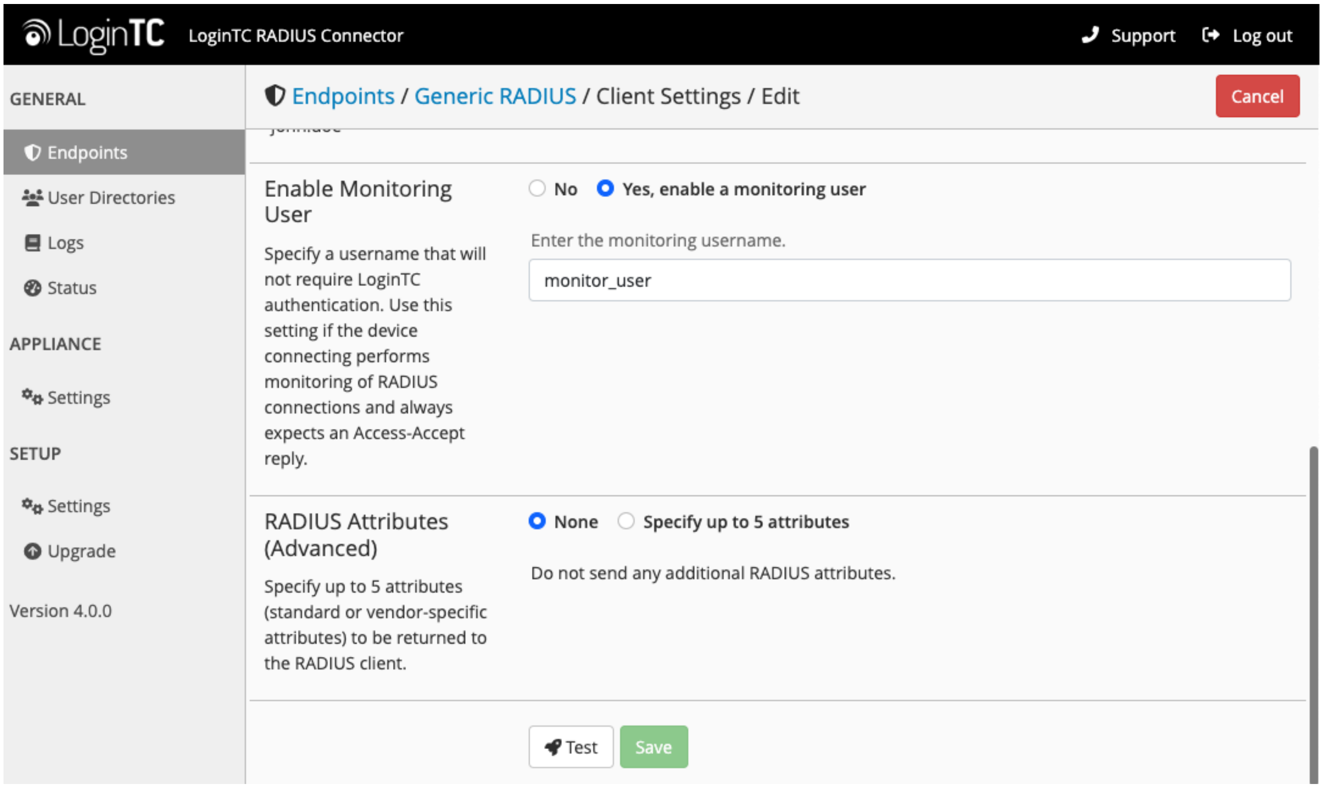


Select the method you wish to use to authenticate and continue.

Loading Balancing and Health Monitoring
Citrix NetScaler allows for multiple LoginTC RADIUS Connectors to be load balanced for high availability.

Steps to configure a health check monitoring user on the LoginTC RADIUS Connector:

1. From the LoginTC RADIUS Connector web based administration page logon using `logintc-user`
2. Click **Configurations**
3. Click on your configuration
4. Scroll down to **Client Settings** and click **Edit**
5. Ensure the **IP Address** matches the correct IP Address. May need to create a new configuration dedicated to monitoring if the health check IP Address does not match the IP Address RADIUS authentication calls originate from.
6. Scroll down to **Enable Monitoring User** and select **Yes, enable a monitoring user**



Endpoints / Generic RADIUS / Client Settings / Edit

Enable Monitoring User

Specify a username that will not require LoginTC authentication. Use this setting if the device connecting performs monitoring of RADIUS connections and always expects an Access-Accept reply.

○ No ● Yes, enable a monitoring user

Enter the monitoring username.

monitor_user

RADIUS Attributes (Advanced)

Specify up to 5 attributes (standard or vendor-specific attributes) to be returned to the RADIUS client.

● None ○ Specify up to 5 attributes

Do not send any additional RADIUS attributes.

7. Enter a **Monitoring Username** that matches the configured monitor in Citrix
8. Click **Test** to validate the values and then click **Save**.

When health checks requests are received for the monitoring user, the configured First Factor authentication will be checked and LoginTC verification will automatically passthrough. If First Factor authentication passes `ACCESS-ACCEPT` will be returned.

LoginTC application dedicated for monitoring

Recommend creating a new LoginTC application and domain only for monitoring. No users need to be part of the application / domain.

(Optional) Active Directory check for monitoring user

Recommend leveraging a dedicated service account for First Factor authentication.

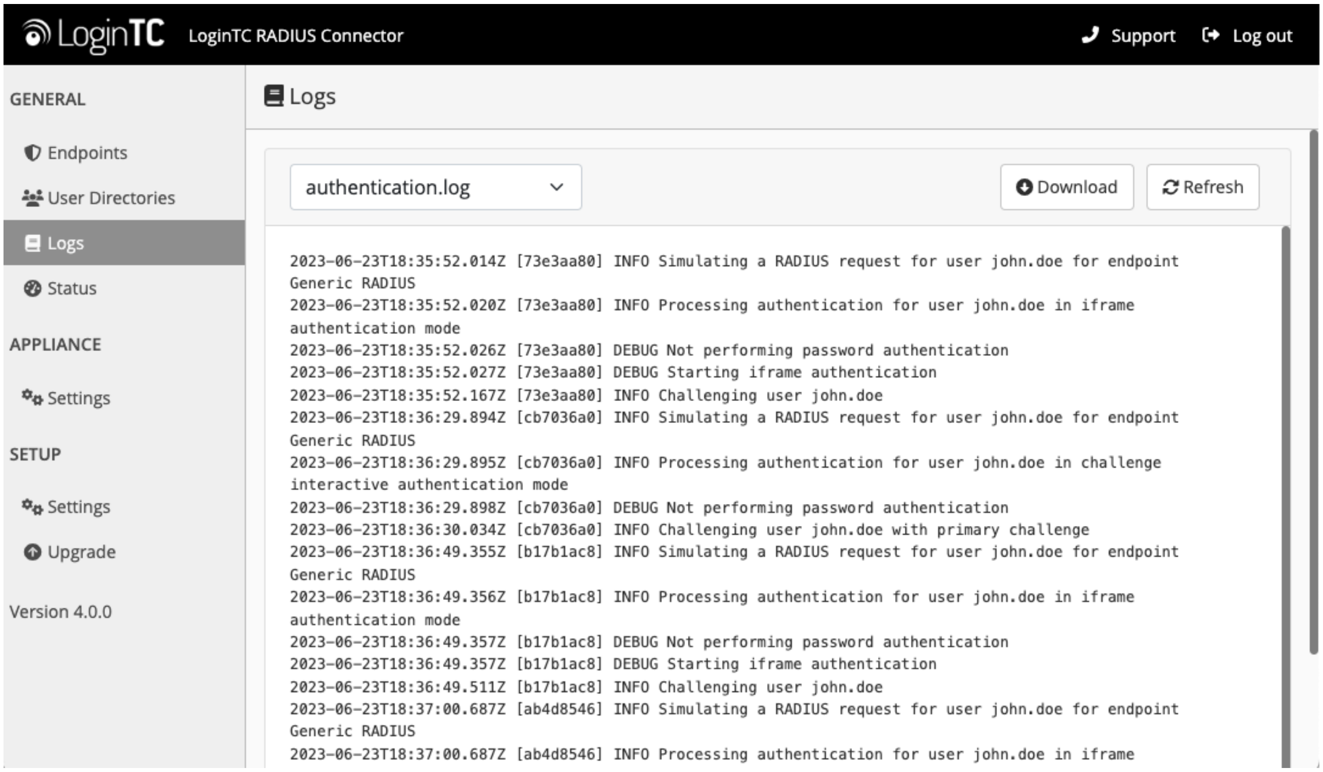
User Management

There are several options for managing your users within LoginTC:

- Individual users can be added manually in LoginTC Admin Panel
- Bulk operations using CSV Import
- Programmatically manage user lifecycle with the REST API
- One-way user synchronization of users to the LoginTC Admin is performed using User Sync Tool.

Logging

Logs can be found on the **Logs** tab:

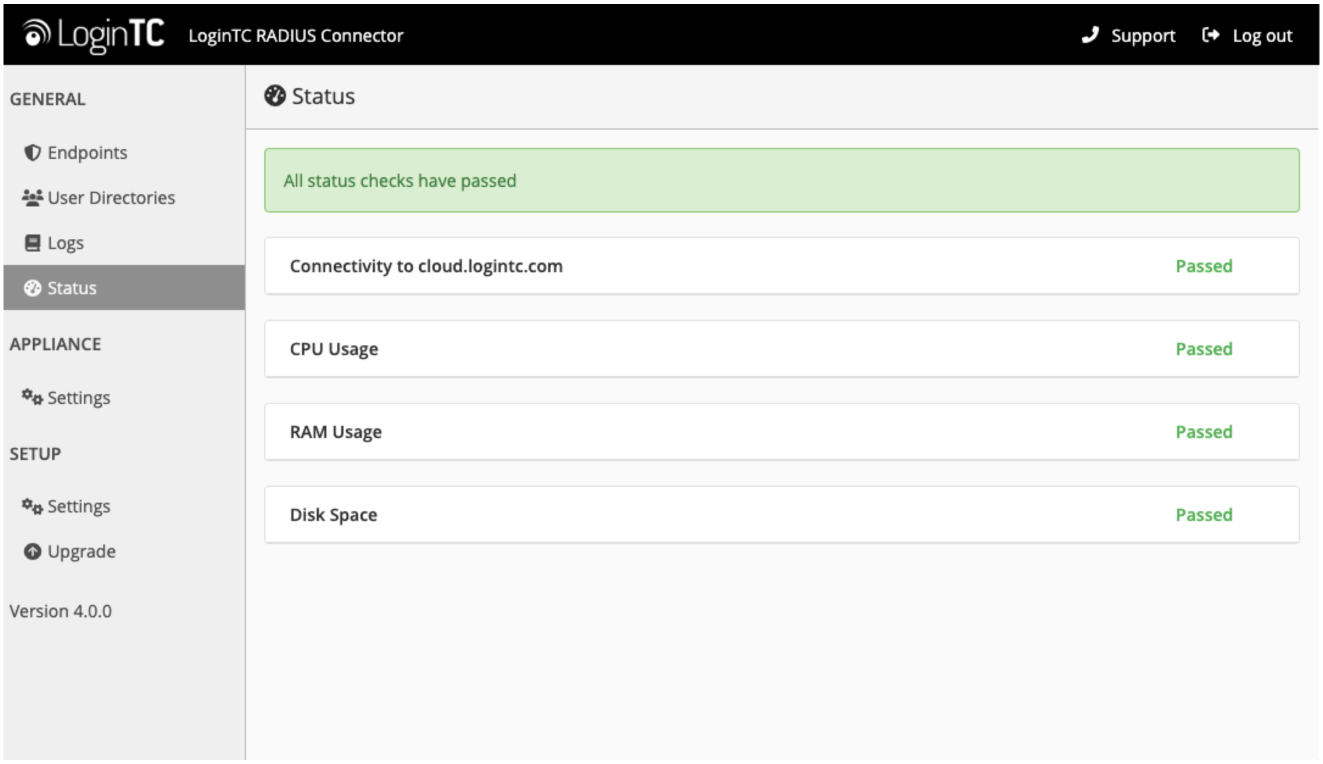


```
2023-06-23T18:35:52.014Z [73e3aa80] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:35:52.020Z [73e3aa80] INFO Processing authentication for user john.doe in iframe
authentication mode
2023-06-23T18:35:52.026Z [73e3aa80] DEBUG Not performing password authentication
2023-06-23T18:35:52.027Z [73e3aa80] DEBUG Starting iframe authentication
2023-06-23T18:35:52.167Z [73e3aa80] INFO Challenging user john.doe
2023-06-23T18:36:29.894Z [cb7036a0] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:36:29.895Z [cb7036a0] INFO Processing authentication for user john.doe in challenge
interactive authentication mode
2023-06-23T18:36:29.898Z [cb7036a0] DEBUG Not performing password authentication
2023-06-23T18:36:30.034Z [cb7036a0] INFO Challenging user john.doe with primary challenge
2023-06-23T18:36:49.355Z [b17b1ac8] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:36:49.356Z [b17b1ac8] INFO Processing authentication for user john.doe in iframe
authentication mode
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Not performing password authentication
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Starting iframe authentication
2023-06-23T18:36:49.511Z [b17b1ac8] INFO Challenging user john.doe
2023-06-23T18:37:00.687Z [ab4d8546] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:37:00.687Z [ab4d8546] INFO Processing authentication for user john.doe in iframe
```

Troubleshooting

Not Authenticating

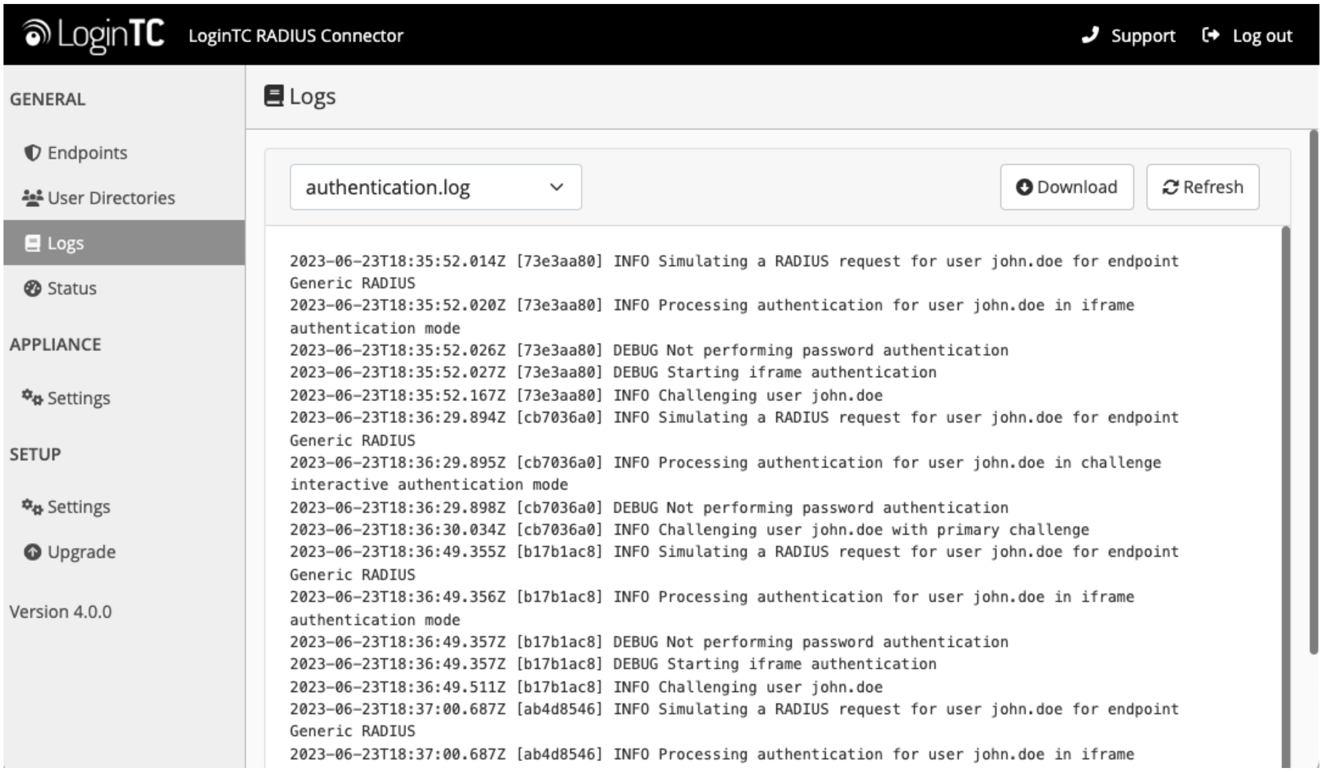
If you are unable to authenticate, navigate to your appliance **web interface** URL and click **Status**:



All status checks have passed

Connectivity to cloud.logintc.com	Passed
CPU Usage	Passed
RAM Usage	Passed
Disk Space	Passed

Ensure that all the status checks pass. For additional troubleshooting, click **Logs**:



```
2023-06-23T18:35:52.014Z [73e3aa80] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:35:52.020Z [73e3aa80] INFO Processing authentication for user john.doe in iframe
authentication mode
2023-06-23T18:35:52.026Z [73e3aa80] DEBUG Not performing password authentication
2023-06-23T18:35:52.027Z [73e3aa80] DEBUG Starting iframe authentication
2023-06-23T18:35:52.167Z [73e3aa80] INFO Challenging user john.doe
2023-06-23T18:36:29.894Z [cb7036a0] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:36:29.895Z [cb7036a0] INFO Processing authentication for user john.doe in challenge
interactive authentication mode
2023-06-23T18:36:29.898Z [cb7036a0] DEBUG Not performing password authentication
2023-06-23T18:36:30.034Z [cb7036a0] INFO Challenging user john.doe with primary challenge
2023-06-23T18:36:49.355Z [b17b1ac8] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:36:49.356Z [b17b1ac8] INFO Processing authentication for user john.doe in iframe
authentication mode
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Not performing password authentication
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Starting iframe authentication
2023-06-23T18:36:49.511Z [b17b1ac8] INFO Challenging user john.doe
2023-06-23T18:37:00.687Z [ab4d8546] INFO Simulating a RADIUS request for user john.doe for endpoint
Generic RADIUS
2023-06-23T18:37:00.687Z [ab4d8546] INFO Processing authentication for user john.doe in iframe
```

Email Support
For any additional help please email support@cyphercor.com. Expect a speedy reply.

Upgrading

From 4.X

The latest LoginTC RADIUS Connector upgrade package can be downloaded here: Download RADIUS Connector (Upgrade)

1. Navigate to **SETUP > Upgrade**:
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:
3. Click **Upload** and do not navigate away from the page:
4. Once upload is complete upgrade by clicking **Install Now**:
5. Wait 10-15 minutes for upgrade to complete:

NOTE: Upgrade time
Upgrade can take 10-15 minutes, please be patient.

From 3.X

Important: LoginTC RADIUS Connector 3.X End-of-life
The LoginTC RADIUS Connector 3.X virtual appliance is built with CentOS 7.9. CentOS 7.X is End of Lifetime (EOL) June 30th, 2024. See CentOS Product Specifications. Although the appliance will still function it will no longer receive updates and nor will it be officially supported.

New LoginTC RADIUS Connector 4.X
A new LoginTC RADIUS Connector 4.X virtual appliance has been created. The Operating System will be supported for many years. Inline upgrade is not supported. As a result upgrade is deploying a new appliance. The appliance has been significantly revamped and although the underlying functionality is identical, it has many new features to take advantage of.

Complete 3.X to 4.X upgrade guide: LoginTC RADIUS Connector Upgrade Guide