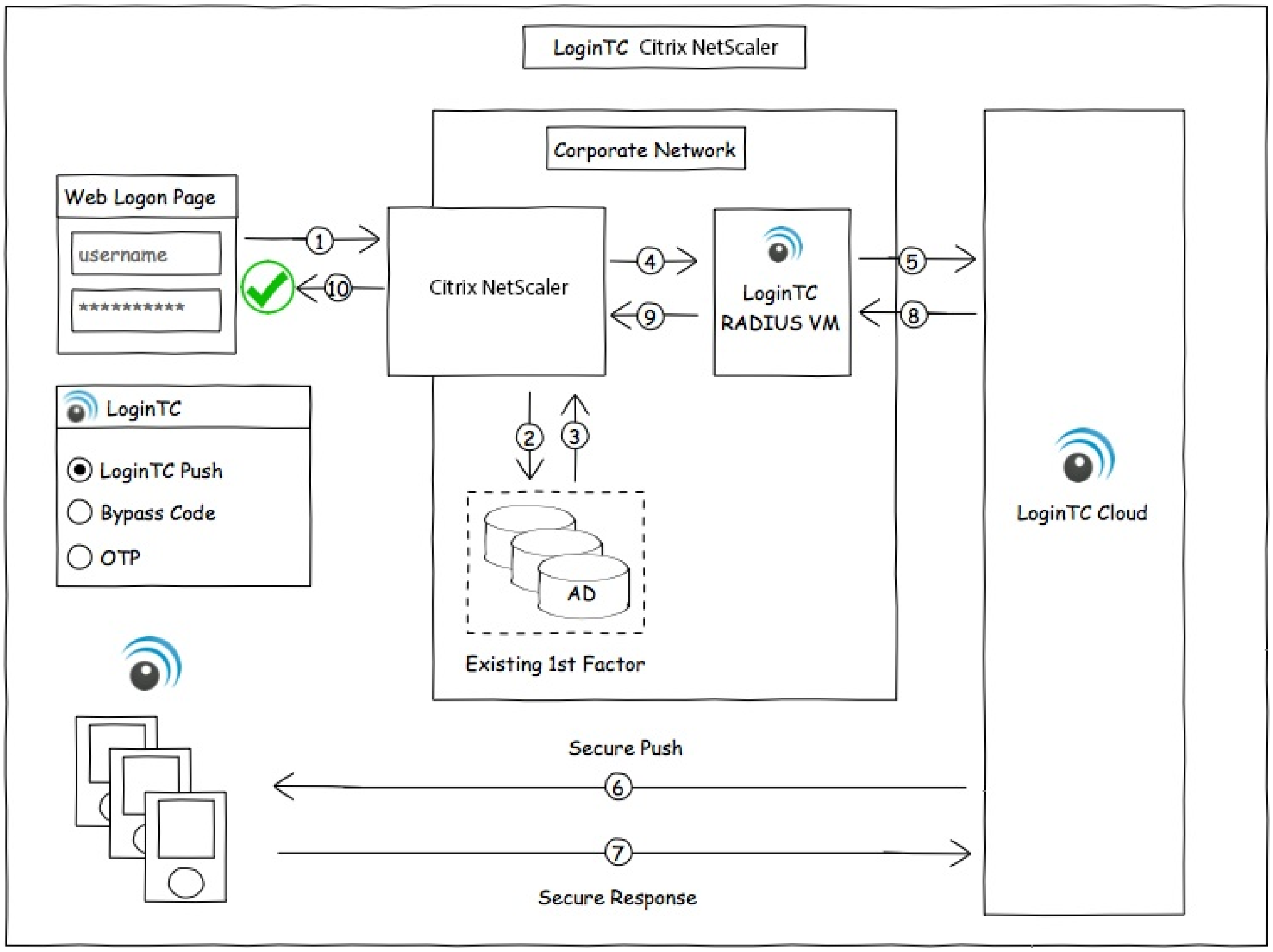
Two factor authentication for Citrix NetScaler

logintc.com/docs/connectors/citrix-netscaler.html

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.



User Experience

After entering the username and password into the Citrix login, the user is shown a selection of second factor options. The user clicks a button to receive a LoginTC push notification, authenticates and is logged in.

Prerequisites

Before proceeding, please ensure you have the following:

LoginTC RADIUS Connector supported version: 2.5.0 or higher

In order to leverage the iframe based solution for Citrix NetScaler please upgrade to 2.5.0 or higher.

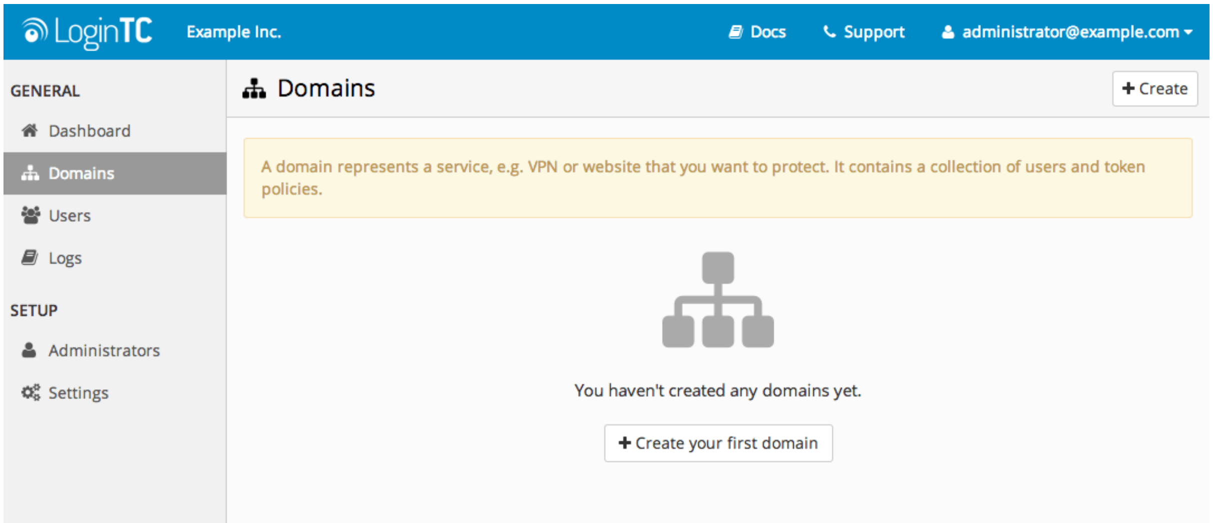
Subscription Requirement

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.

RADIUS Domain Creation

If you have already created a LoginTC Admin domain for your LoginTC RADIUS Connector, then you may skip this section and proceed to Installation.

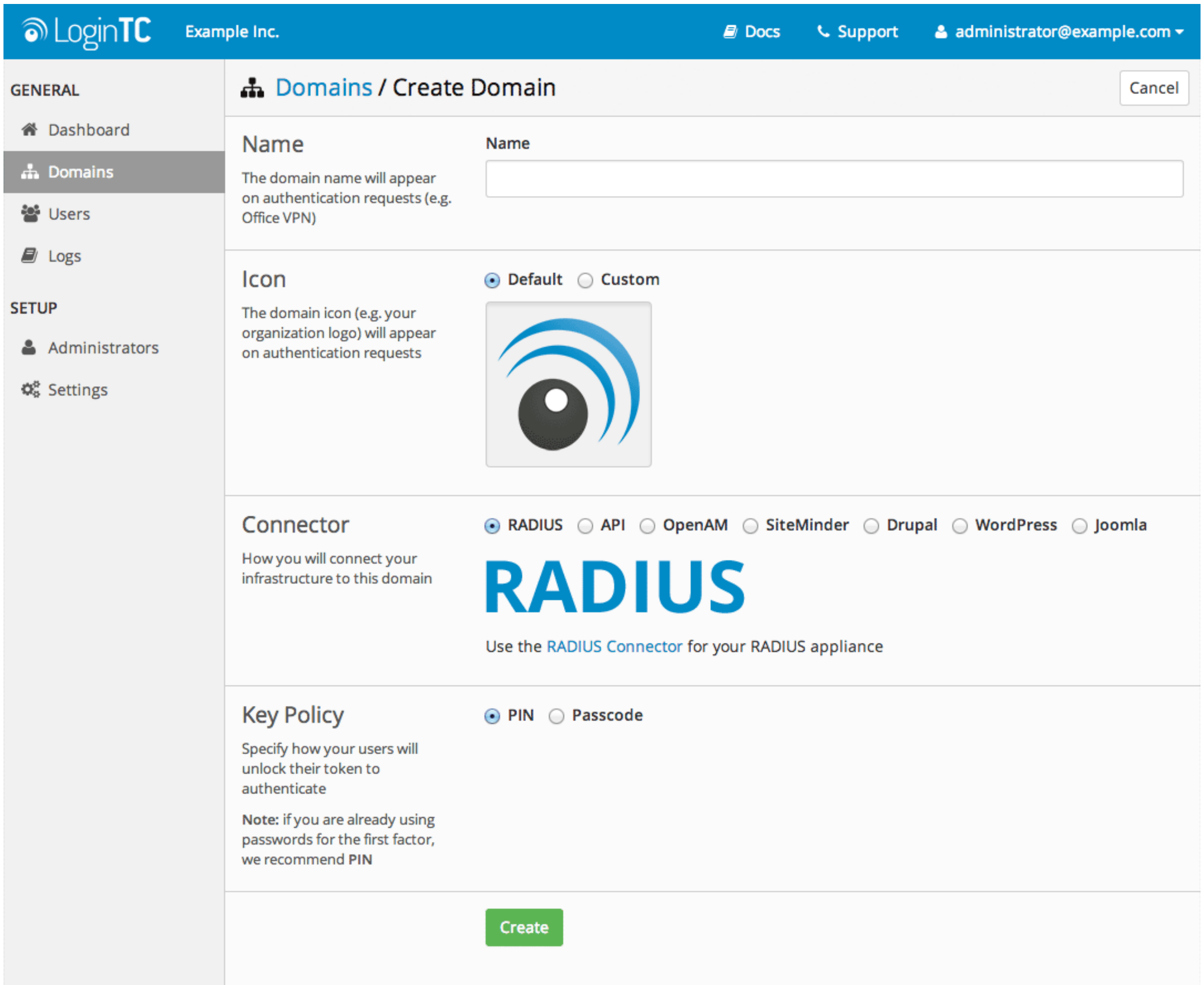
1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Add Domain**:



A domain represents a service, e.g. VPN or website that you want to protect. It contains a collection of users and token policies.

You haven't created any domains yet.

4. Enter domain information:



Domains / Create Domain

Name

The domain name will appear on authentication requests (e.g. Office VPN)

Name:

Icon

The domain icon (e.g. your organization logo) will appear on authentication requests

● Default ○ Custom

Connector

How you will connect your infrastructure to this domain

● RADIUS ○ API ○ OpenAM ○ SiteMinder ○ Drupal ○ WordPress ○ Joomla

RADIUS

Use the RADIUS Connector for your RADIUS appliance

Key Policy

Specify how your users will unlock their token to authenticate

Note: if you are already using passwords for the first factor, we recommend **PIN**

● PIN ○ Passcode

Name
Choose a name to identify your LoginTC Admin domain to you and your users

Connector
RADIUS

Installation

The LoginTC RADIUS Connector runs CentOS 6.8 with SELinux. A firewall runs with the following open ports:

Port	Protocol	Purpose
22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
443	TCP	Web interface
80	TCP	Web interface
80	TCP	Package updates (outgoing)

Port	Protocol	Purpose
123	UDP	NTP, Clock synchronization (outgoing)

No incoming traffic rules required

The LoginTC RADIUS Connector is designed to work within your network without the need to change incoming rules on your firewall.

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 and will not be able to access the **web interface** unless it is changed.

The `logintc-user` has `sudo` privileges.

Configuration

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

1. LoginTC

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

2. First Factor

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 (since there are 4-digit PIN and Passcode options that unlock the tokens to access your domains, LoginTC-only authentication this still provides two-factor authentication).

3. 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 and Encryption

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

Data Encryption

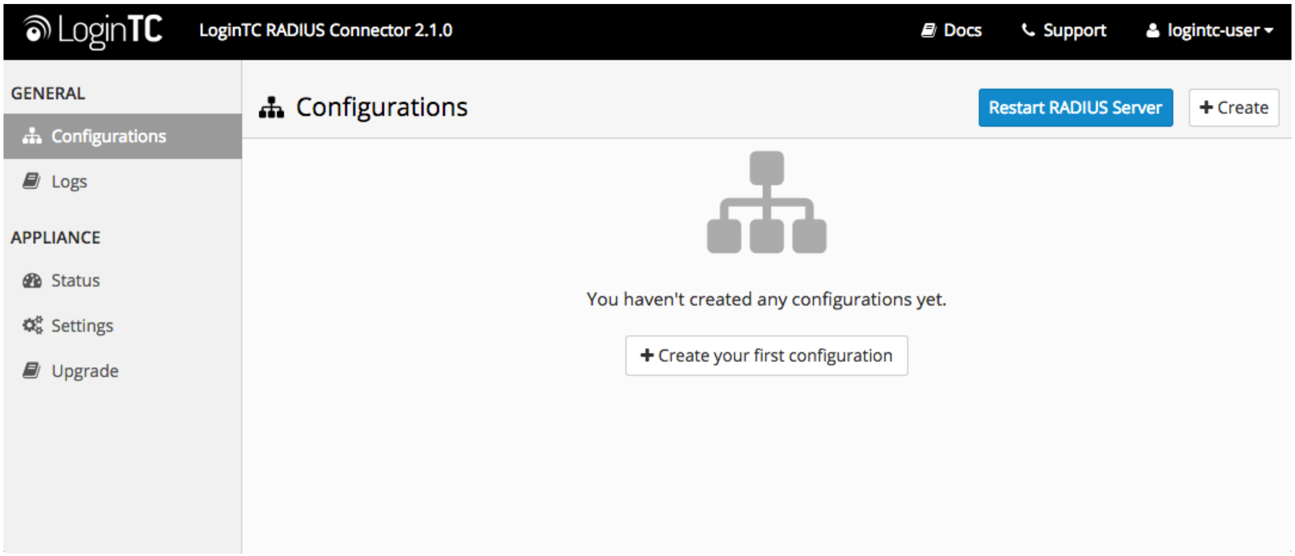
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

The **web interface** makes setting up a configuration 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 Configuration

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.

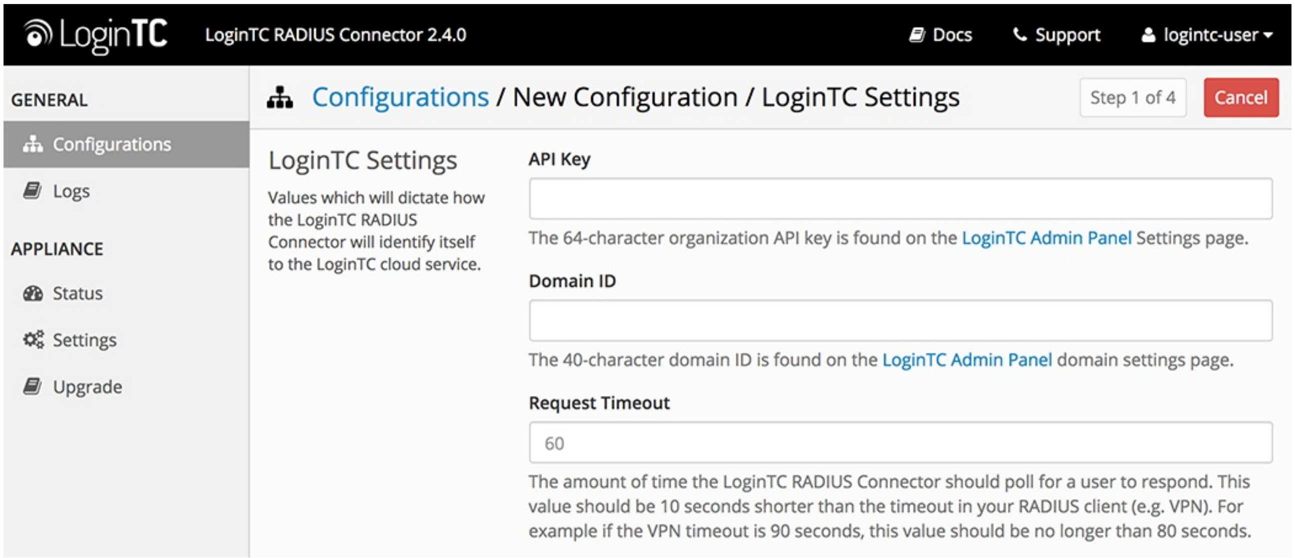
Create a new configuration file by clicking **+ Create your first configuration**:



You haven't created any configurations yet.

LoginTC Settings

Configure which LoginTC organization and domain to use:



Configurations / New Configuration / LoginTC Settings

LoginTC Settings

Values which will dictate how the LoginTC RADIUS Connector will identify itself to the LoginTC cloud service.

API Key

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

Domain ID

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

Request Timeout

60

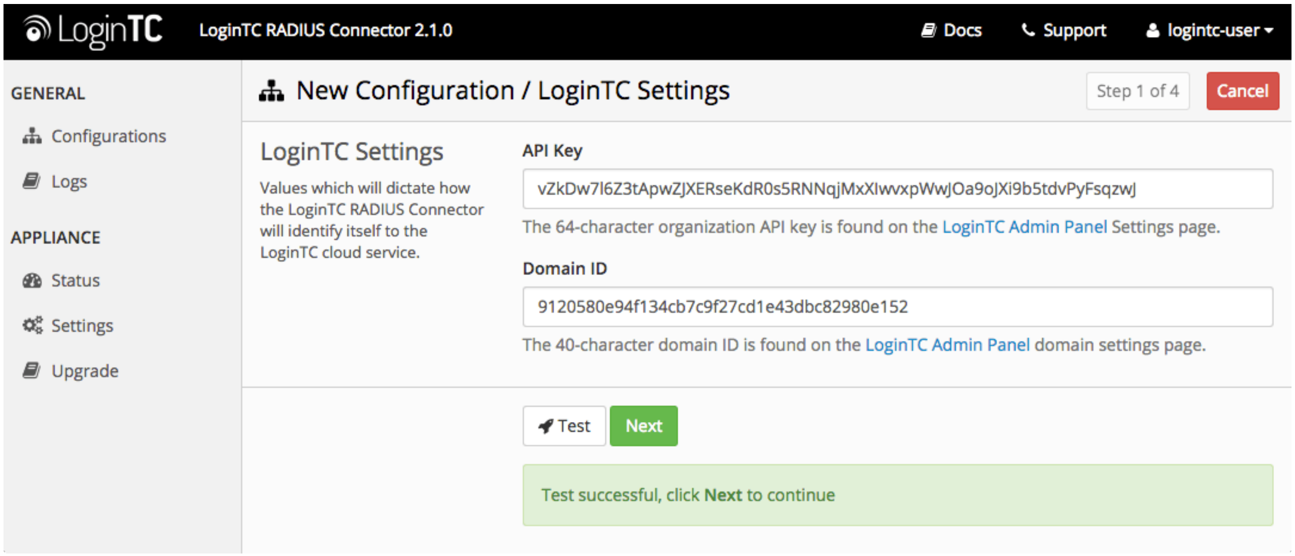
The amount of time the LoginTC RADIUS Connector should poll for a user to respond. This value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

Configuration values:

Property	Explanation
`api_key`	The 64-character organization API key
`domain_id`	The 40-character domain ID

The API key is found on the LoginTC Admin Settings page. The Domain ID is found on your domain settings page.

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



New Configuration / LoginTC Settings

LoginTC Settings

Values which will dictate how the LoginTC RADIUS Connector will identify itself to the LoginTC cloud service.

API Key

vZkDw7l6Z3tApwZJXERseKdR0s5RNNqjMxXIwvxpWwJOa9oJXi9b5tdvPyFsqzwJ

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

Domain ID

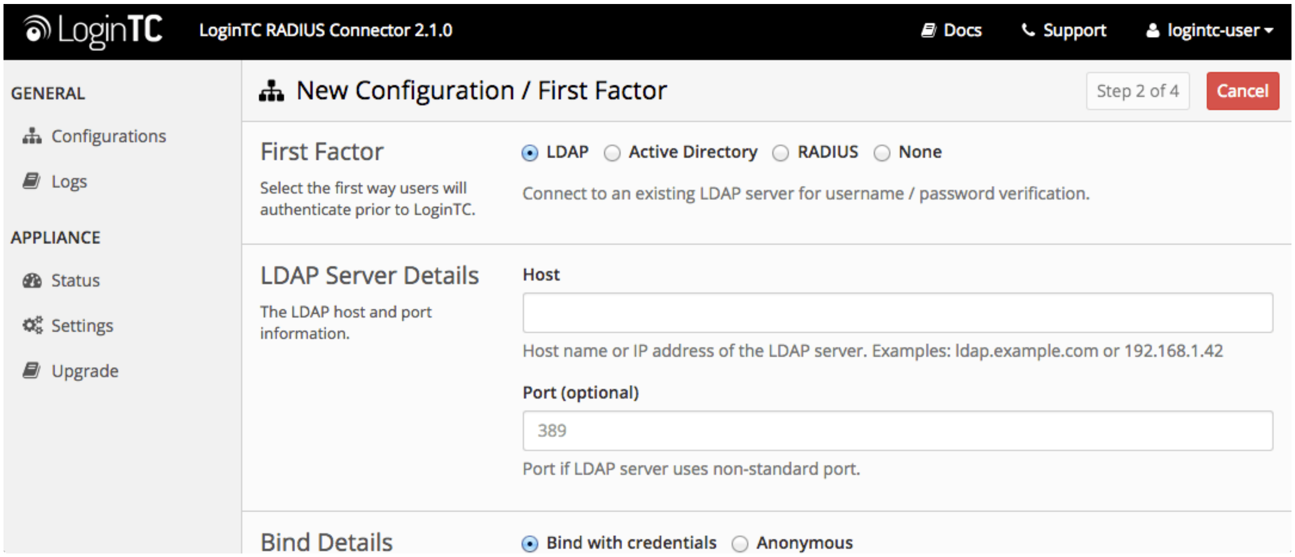
9120580e94f134cb7c9f27cd1e43dbc82980e152

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

Test successful, click **Next** to continue

First Authentication Factor

Configure the first authentication factor to be used 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.



New Configuration / First Factor

First Factor

Select the first way users will authenticate prior to LoginTC.

● LDAP ○ Active Directory ○ RADIUS ○ None

Connect to an existing LDAP server for username / password verification.

LDAP Server Details

The LDAP host and port information.

Host

Host name or IP address of the LDAP server. Examples: ldap.example.com or 192.168.1.42

Port (optional)

389

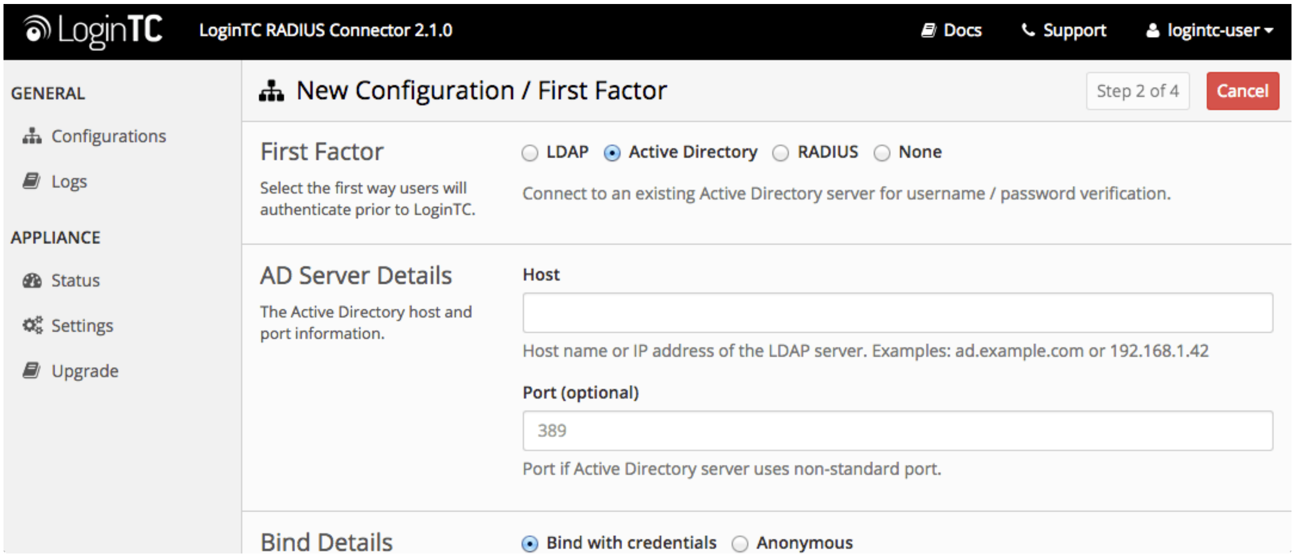
Port if LDAP server uses non-standard port.

Bind Details

● Bind with credentials ○ Anonymous

Active Directory / LDAP Option

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



New Configuration / First Factor

First Factor

Select the first way users will authenticate prior to LoginTC.

○ LDAP ● Active Directory ○ RADIUS ○ None

Connect to an existing Active Directory server for username / password verification.

AD Server Details

The Active Directory host and port information.

Host

Host name or IP address of the LDAP server. Examples: ad.example.com or 192.168.1.42

Port (optional)

389

Port if Active Directory server uses non-standard port.

Bind Details

● Bind with credentials ○ Anonymous

Configuration values:

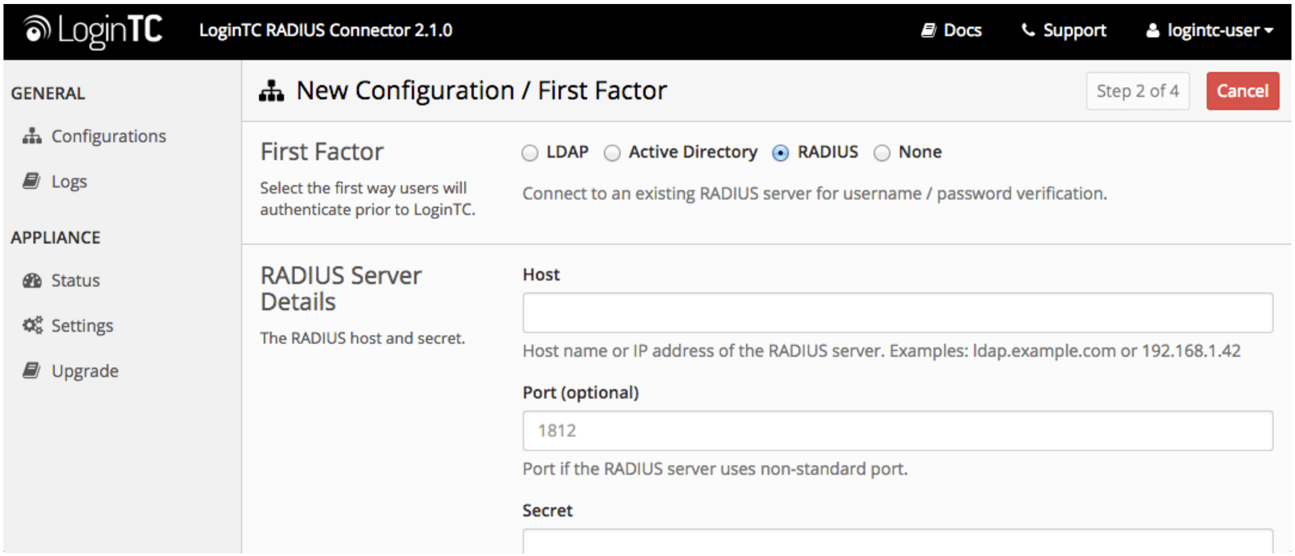
Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The 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`
`Group Attribute` (optional)	Specify an additional user group attribute to be returned the authenticating server.	`4000`
`RADIUS Group Attribute` (optional)	Name of RADIUS attribute to send back	`Filter-Id`
`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**:



New Configuration / First Factor

First Factor

Select the first way users will authenticate prior to LoginTC.

○ LDAP ○ Active Directory ● RADIUS ○ None

Connect to an existing RADIUS server for username / password verification.

RADIUS Server Details

The RADIUS host and secret.

Host

Host name or IP address of the RADIUS server. Examples: ldap.example.com or 192.168.1.42

Port (optional)

1812

Port if the RADIUS server uses non-standard port.

Secret

Configuration values:

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

RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) found in the FreeRADIUS dictionary files will be relayed.

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

Passthrough

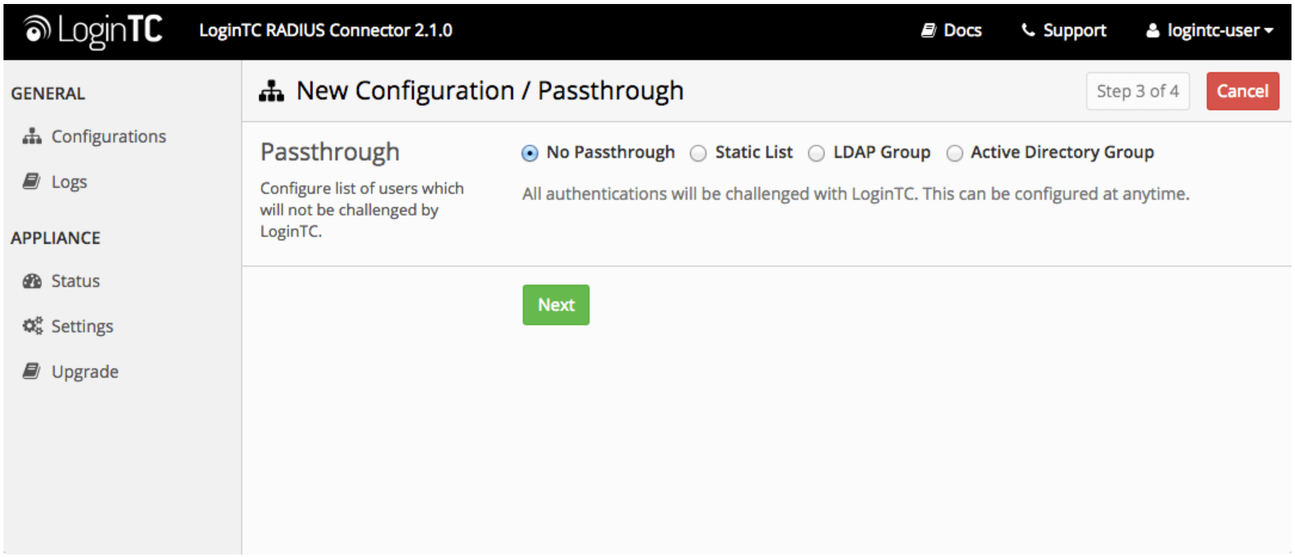
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.

No Passthrough (default)

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



New Configuration / Passthrough

Passthrough

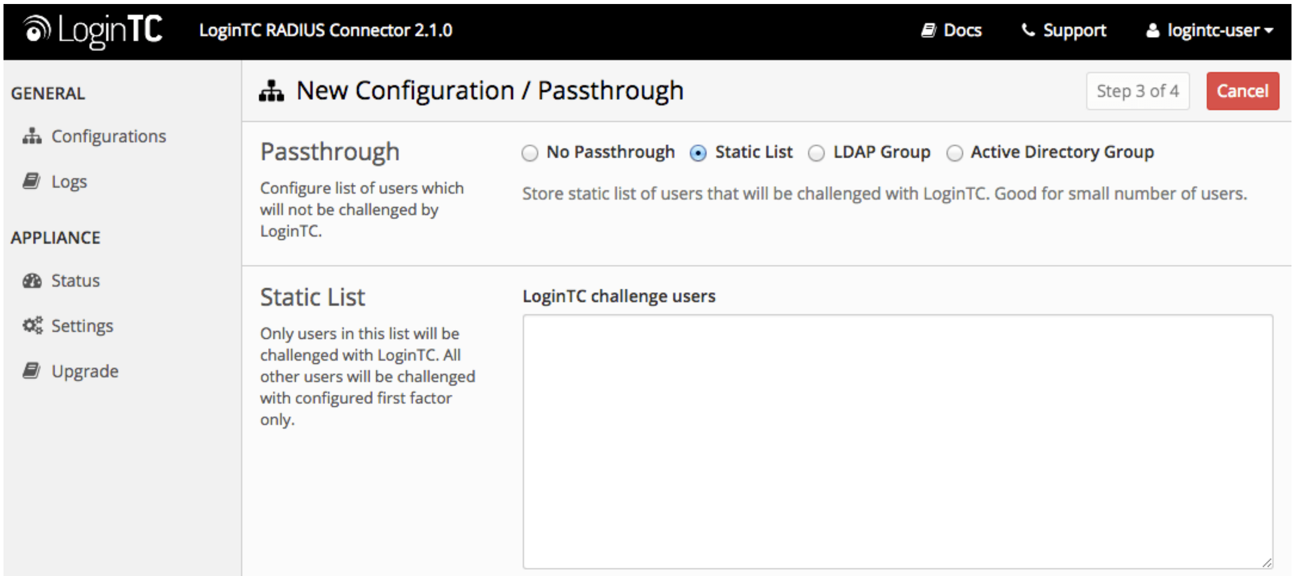
Configure list of users which will not be challenged by LoginTC.

● No Passthrough ○ Static List ○ LDAP Group ○ Active Directory Group

All authentications will be challenged with LoginTC. This can be configured at anytime.

Static 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.



New Configuration / Passthrough

Passthrough

Configure list of users which will not be challenged by LoginTC.

○ No Passthrough ● Static List ○ LDAP Group ○ Active Directory Group

Store static list of users that will be challenged with LoginTC. Good for small number of users.

Static List

Only users in this list will be challenged with LoginTC. All other users will be challenged with configured first factor only.

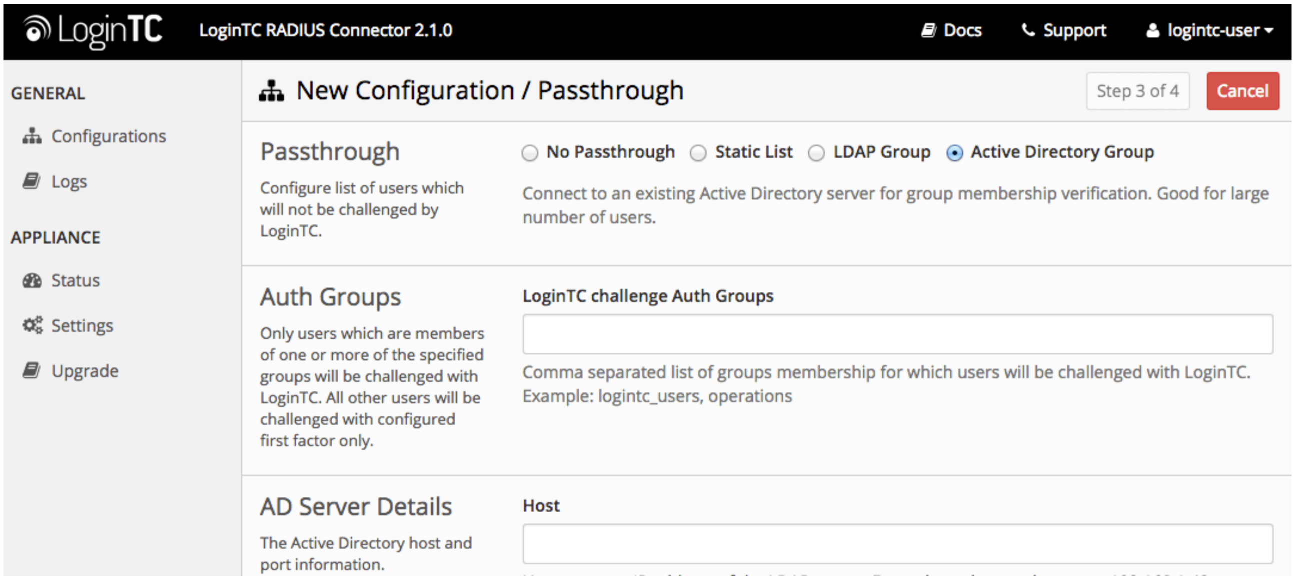
LoginTC challenge users

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

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

Active Directory / LDAP Group

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.



New Configuration / Passthrough

Passthrough

Configure list of users which will not be challenged by LoginTC.

○ No Passthrough ○ Static List ○ LDAP Group ● Active Directory Group

Connect to an existing Active Directory server for group membership verification. Good for large number of users.

Auth Groups

Only users which are members of one or more of the specified groups will be challenged with LoginTC. All other users will be challenged with configured first factor only.

LoginTC challenge Auth Groups

Comma separated list of groups membership for which users will be challenged with LoginTC. Example: logintc_users, operations

AD Server Details

The Active Directory host and port information.

Host

Configuration values:

Property	Explanation	Examples
`LoginTC challenge auth groups`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users` or `two-factor-users`

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`
`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`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

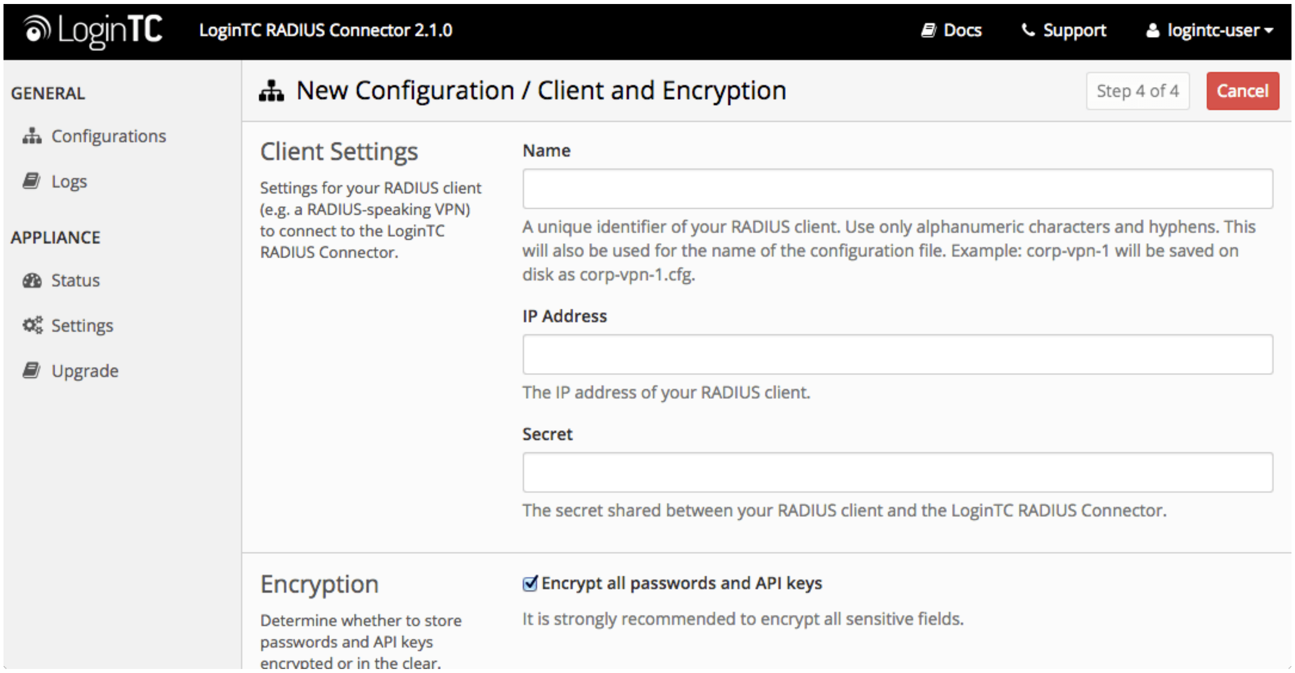
Configuration Simplified

If Active Directory / LDAP Option was selected in First Authentication Factor the non-sensitive values will be pre-populated to avoid retyping and potential typos.

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

Client and Encryption

Configure RADIUS client (e.g. your Citrix NetScaler):



New Configuration / Client and Encryption

Client Settings

Settings for your RADIUS client (e.g. a RADIUS-speaking VPN) to connect to the LoginTC RADIUS Connector.

Name

A unique identifier of your RADIUS client. Use only alphanumeric characters and hyphens. This will also be used for the name of the configuration file. Example: corp-vpn-1 will be saved on disk as corp-vpn-1.cfg.

IP Address

The IP address of your RADIUS client.

Secret

The secret shared between your RADIUS client and the LoginTC RADIUS Connector.

Encryption

Determine whether to store passwords and API keys encrypted or in the clear.

☑ Encrypt all passwords and API keys

It is strongly recommended to encrypt all sensitive fields.

Client configuration values:

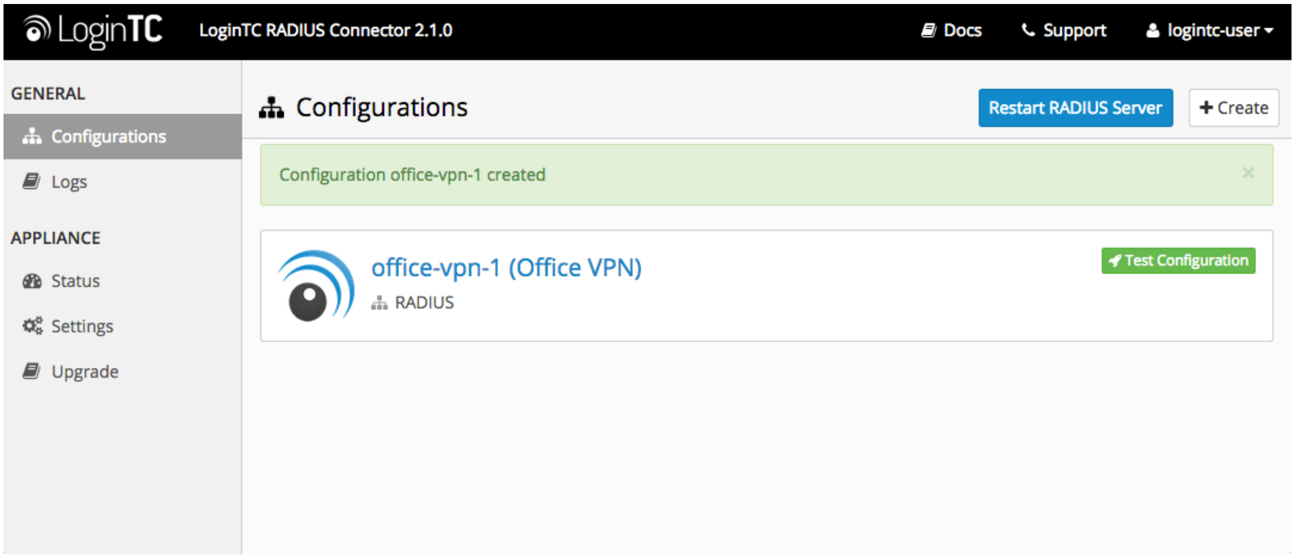
Property	Explanation	Examples
`name`	A unique identifier of your RADIUS client	`CorporateVPN`
`ip`	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	`192.168.1.44`
`secret`	The secret shared between the LoginTC RADIUS Connector and its client	`bigsecret`

The `Authenticate Mode` must be set to `Iframe` .

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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



Configurations

Configuration office-vpn-1 created

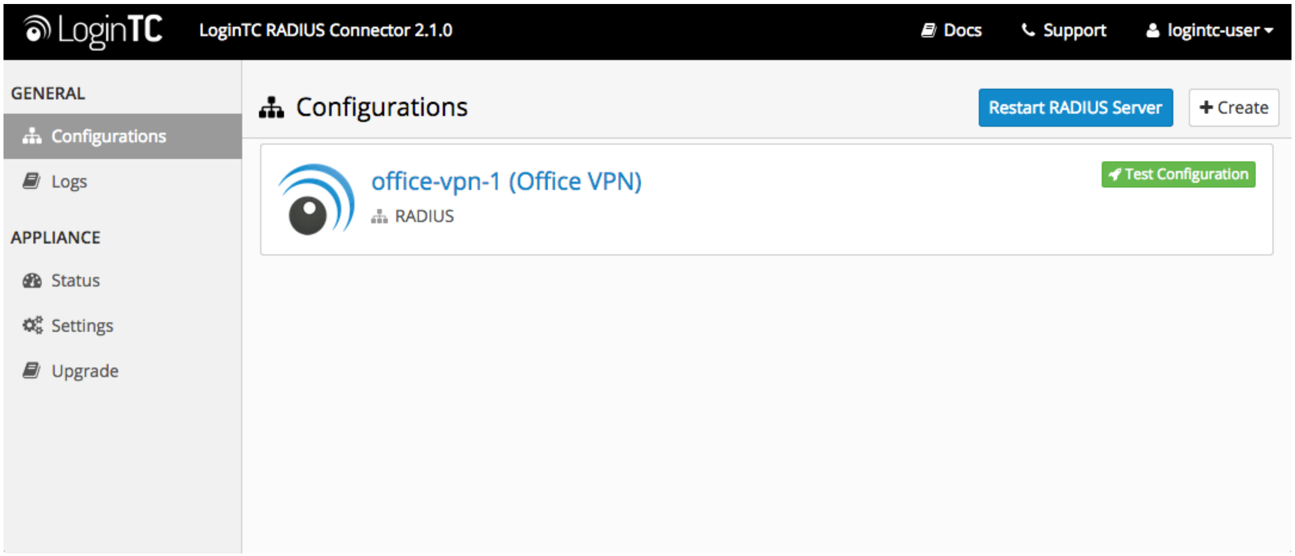
office-vpn-1 (Office VPN)

RADIUS

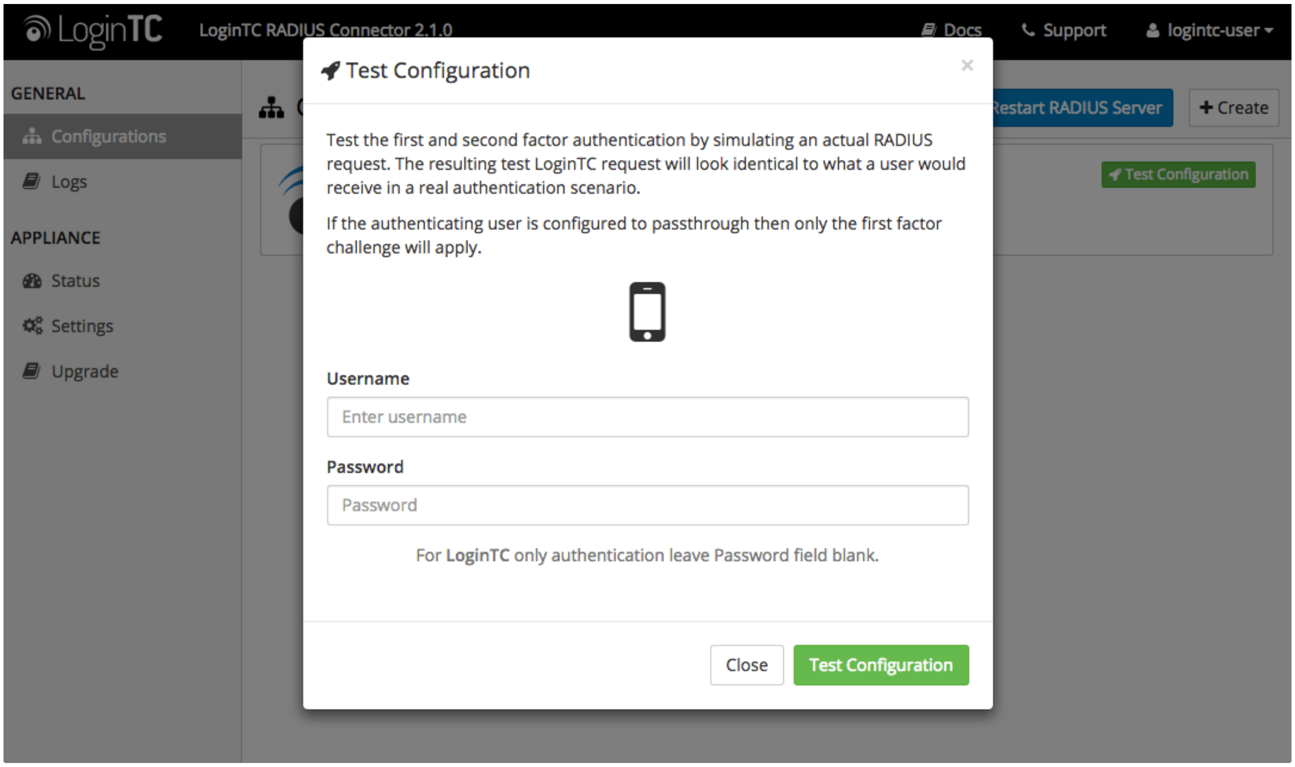
Testing

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:

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



Click **Test Configuration**:

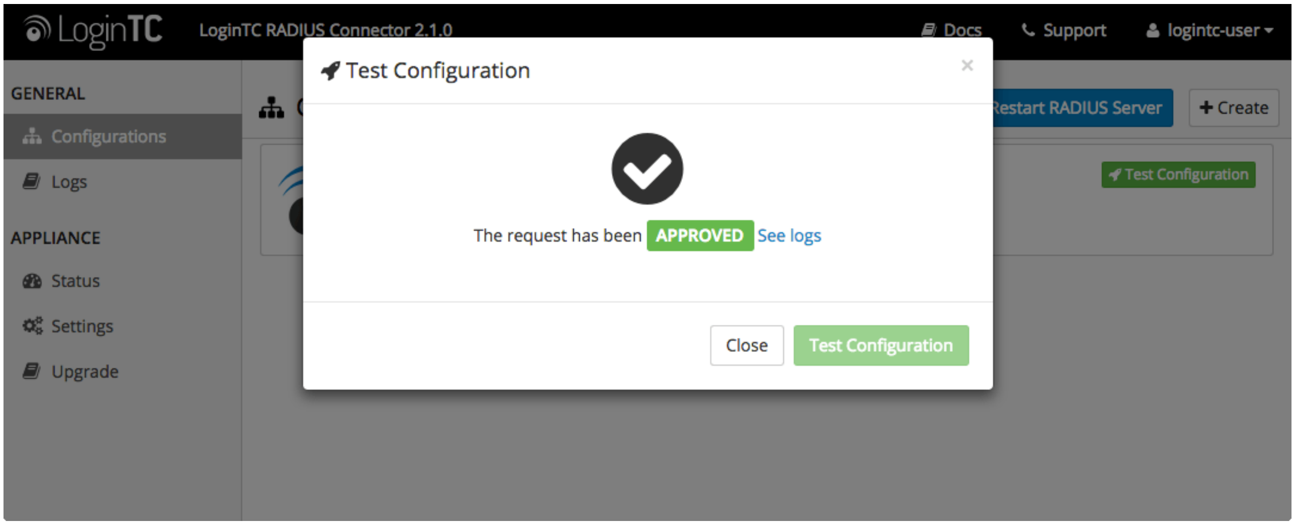


Test the first and second factor authentication by simulating an actual RADIUS request. The resulting test LoginTC request will look identical to what a user would receive in a real authentication scenario.

If the authenticating user is configured to passthrough then only the first factor challenge will apply.

For **LoginTC** only authentication leave Password field blank.

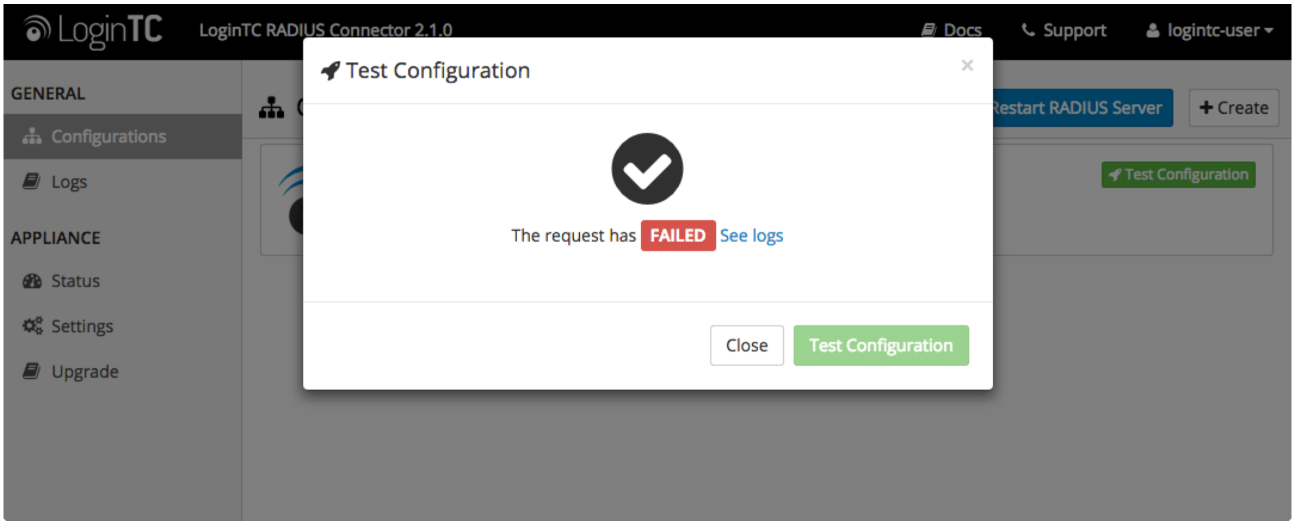
Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:



The request has been APPROVED See logs

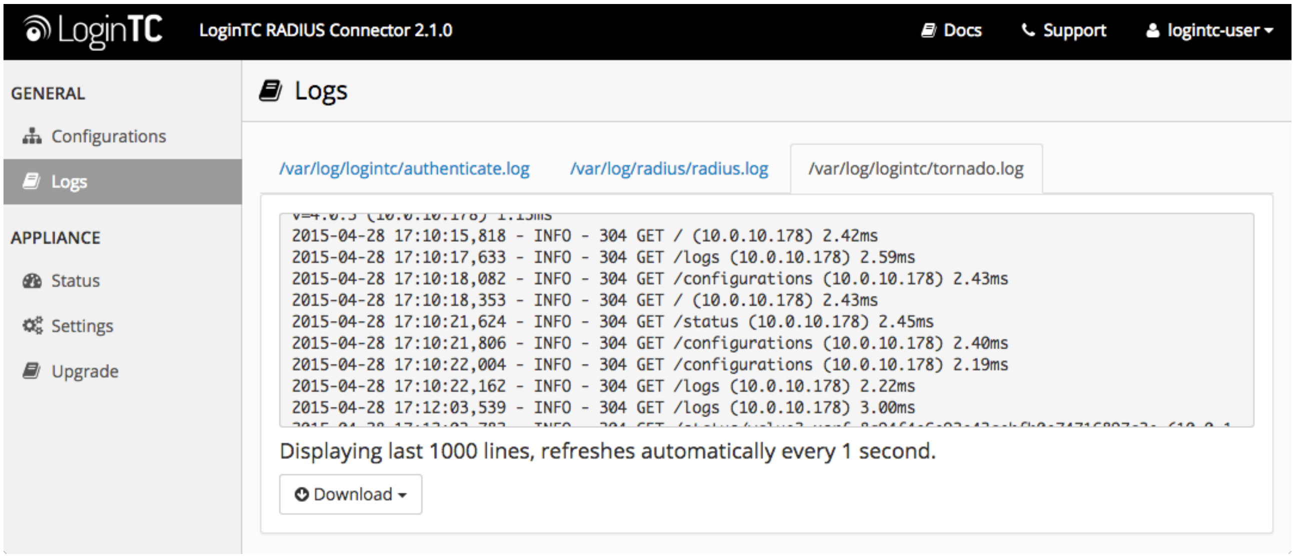
Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



The request has FAILED See logs

In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:


LoginTC
LoginTC RADIUS Connector 2.1.0
Docs
Support
logintc-user
GENERAL
Configurations
Logs
APPLIANCE
Status
Settings
Upgrade
Logs
/var/log/logintc/authenticate.log
/var/log/radius/radius.log
/var/log/logintc/tornado.log
Download

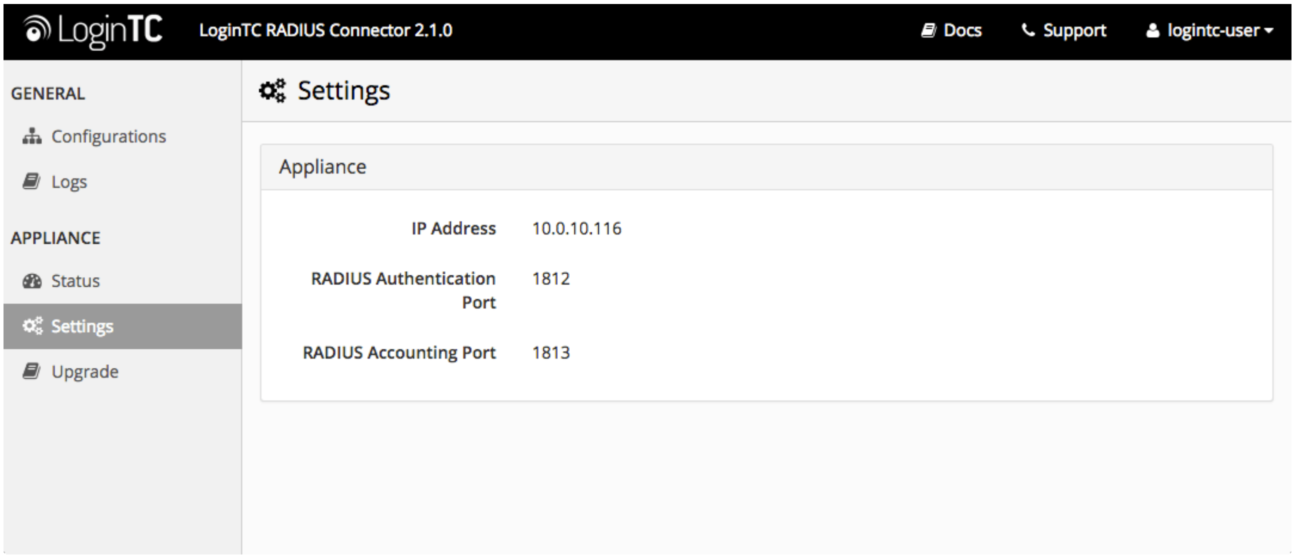
```
v=4.0.5 (10.0.10.178) 1.15ms
2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms
2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms
2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms
2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms
2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms
2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms
2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms
2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms
```

Displaying last 1000 lines, refreshes automatically every 1 second.

Citrix NetScaler Configuration

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

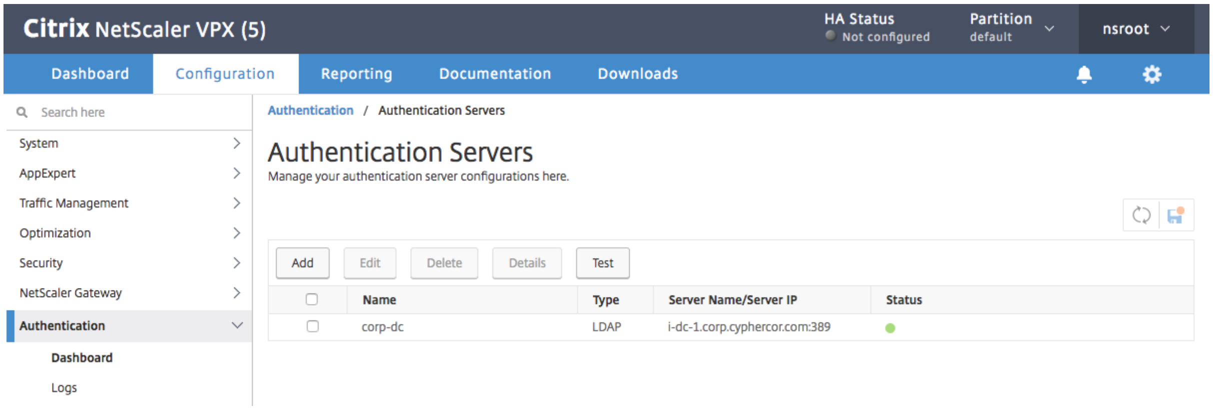
For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:



IP Address	10.0.10.116
RADIUS Authentication Port	1812
RADIUS Accounting Port	1813

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**:

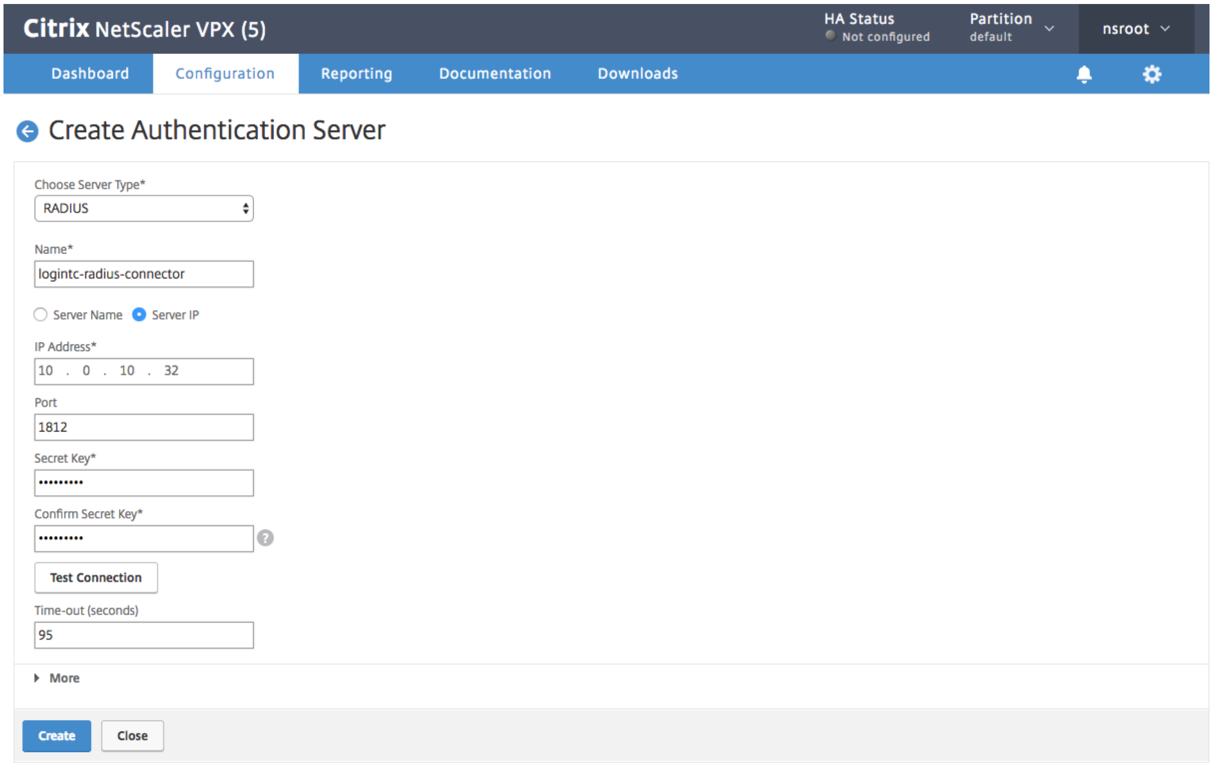


Authentication Servers

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



Choose Server Type*: RADIUS

Name*: logintc-radius-connector

○ Server Name ● Server IP

IP Address*: 10 . 0 . 10 . 32

Port: 1812

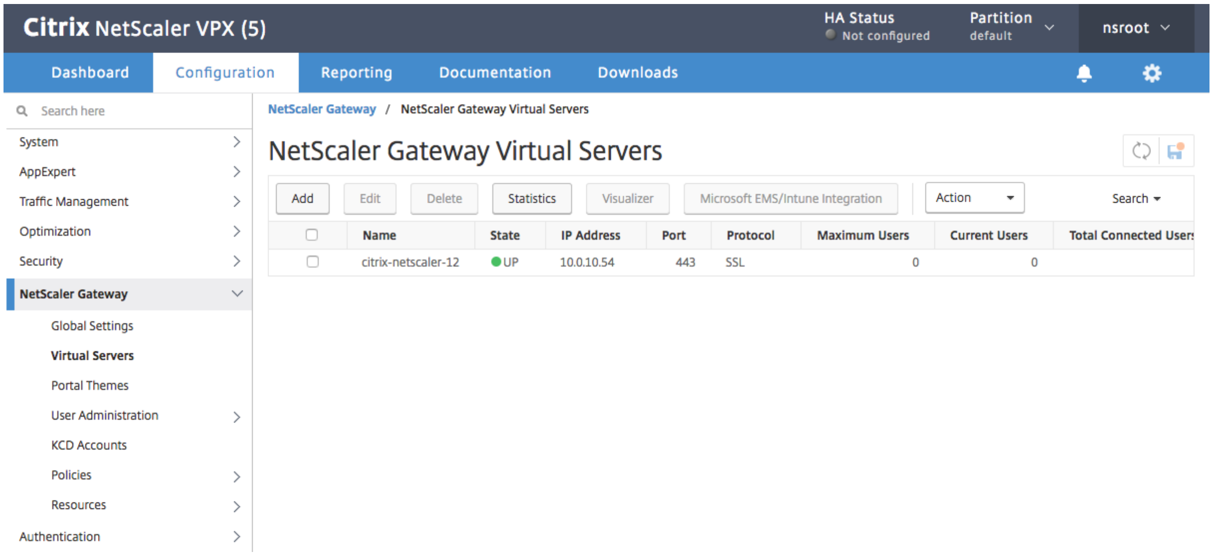
Secret Key*: •••••••••

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`

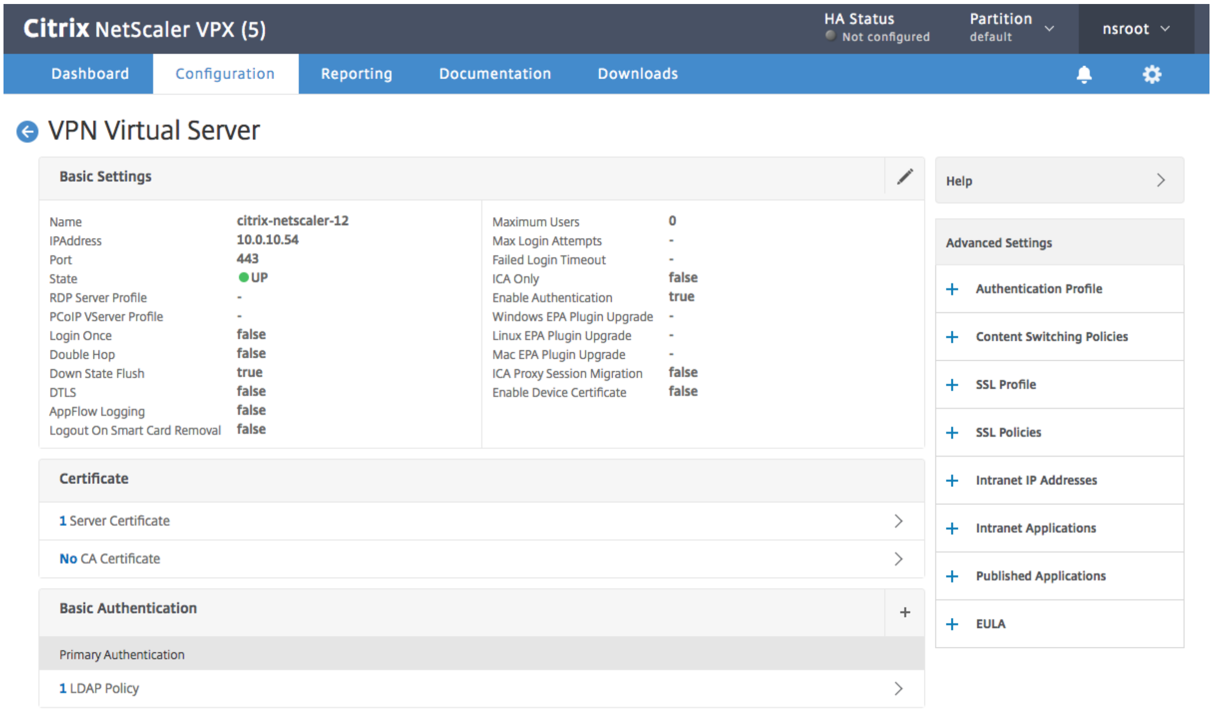
5. Press **Create**
6. Navigate to **NetScaler Gateway** > **Virtual Servers**



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

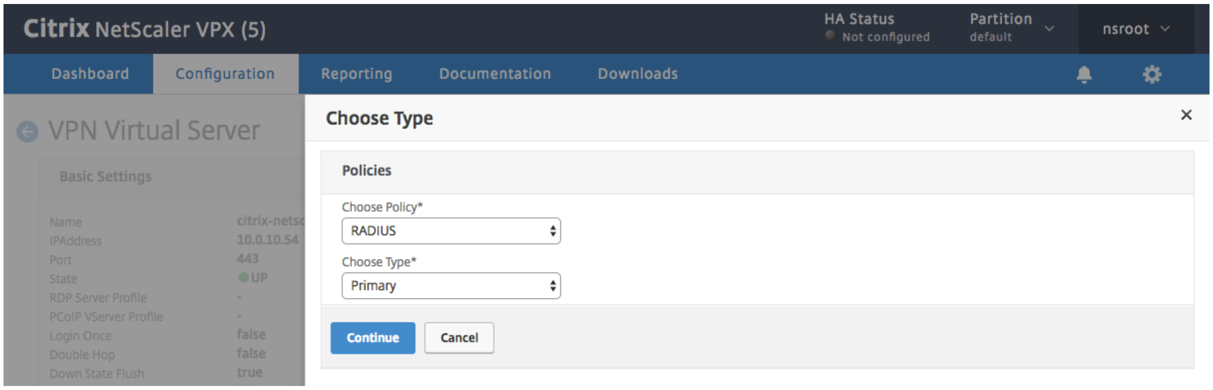
No CA Certificate

Basic Authentication +

Primary Authentication

1 LDAP Policy

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



Choose Type ×

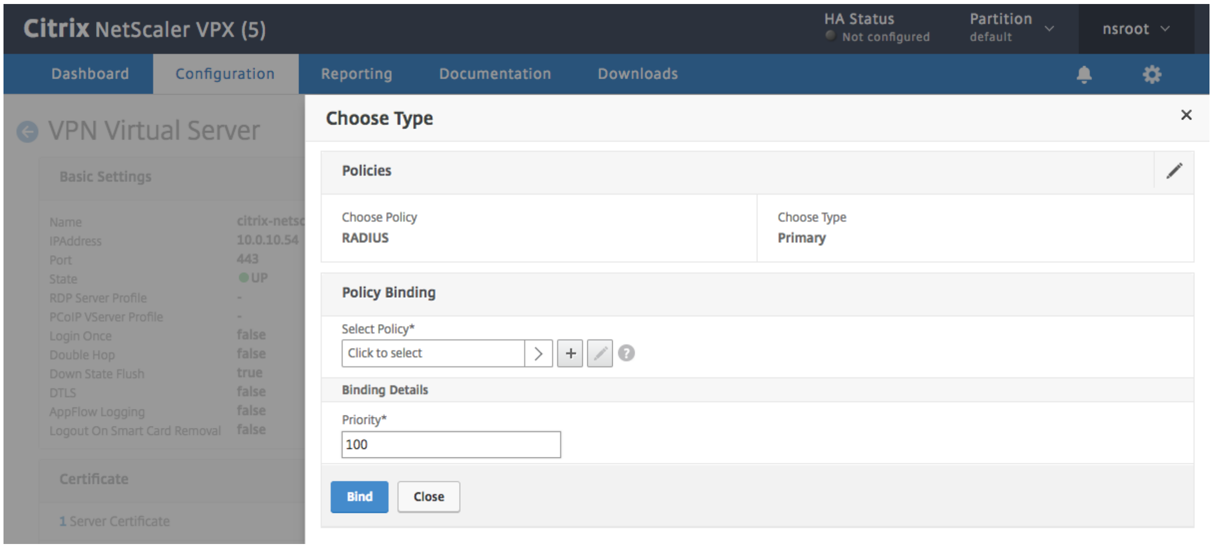
Policies

Choose Policy*: RADIUS

Choose Type*: Primary

10. Press **Continue**

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



Basic Settings

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

Certificate

1 Server Certificate

Choose Type

Policies

Choose Policy: RADIUS

Choose Type: Primary

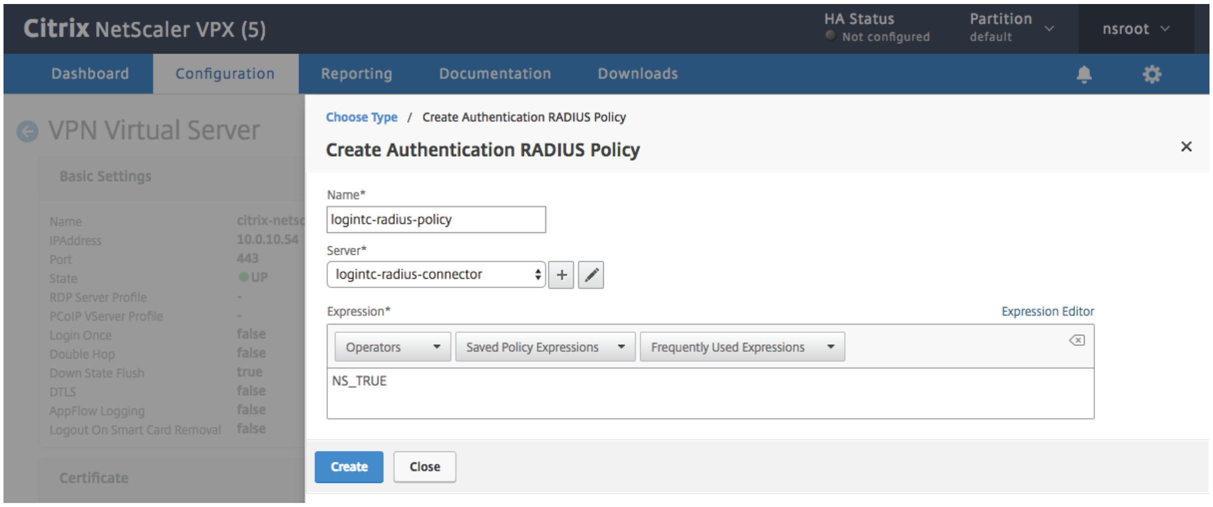
Policy Binding

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



Basic Settings

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

Certificate

Choose Type / Create Authentication RADIUS Policy

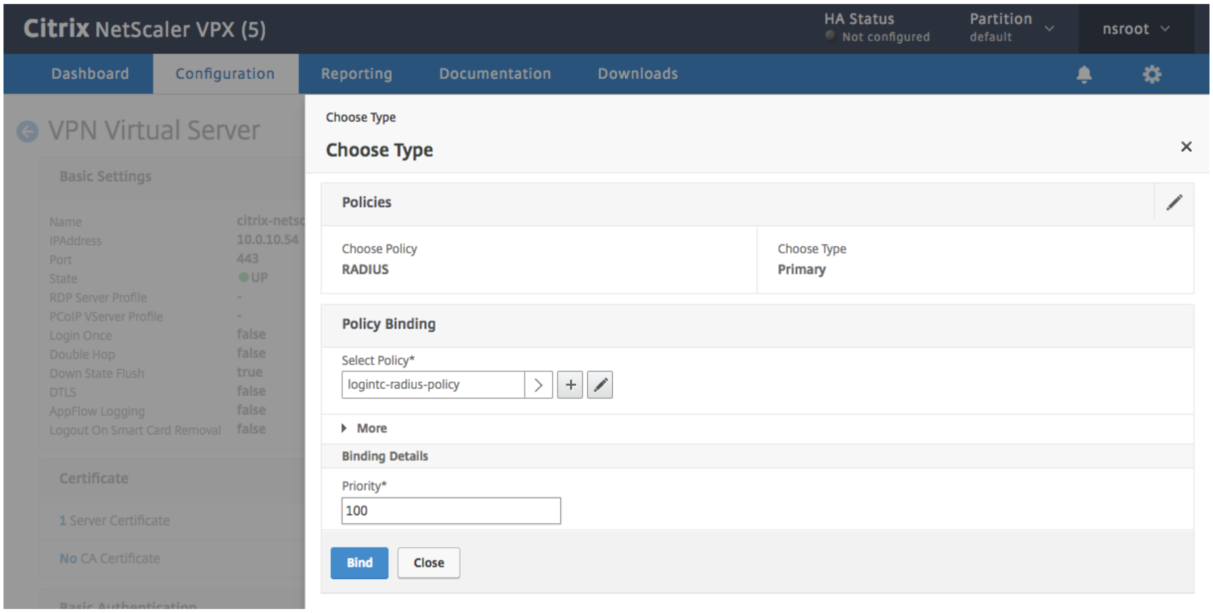
Create Authentication RADIUS Policy

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

1 Server Certificate

No CA Certificate

Choose Type

Choose Type

Policies

Choose Policy	Choose Type
RADIUS	Primary

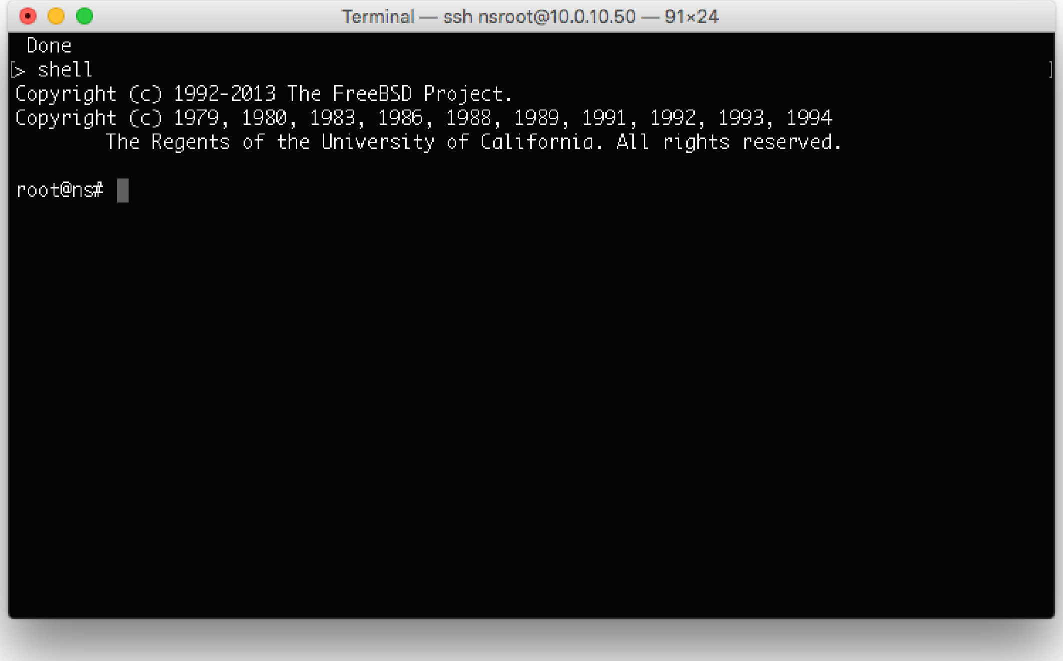
Policy Binding

Select Policy* logintc-radius-policy

Binding Details

Priority* 100

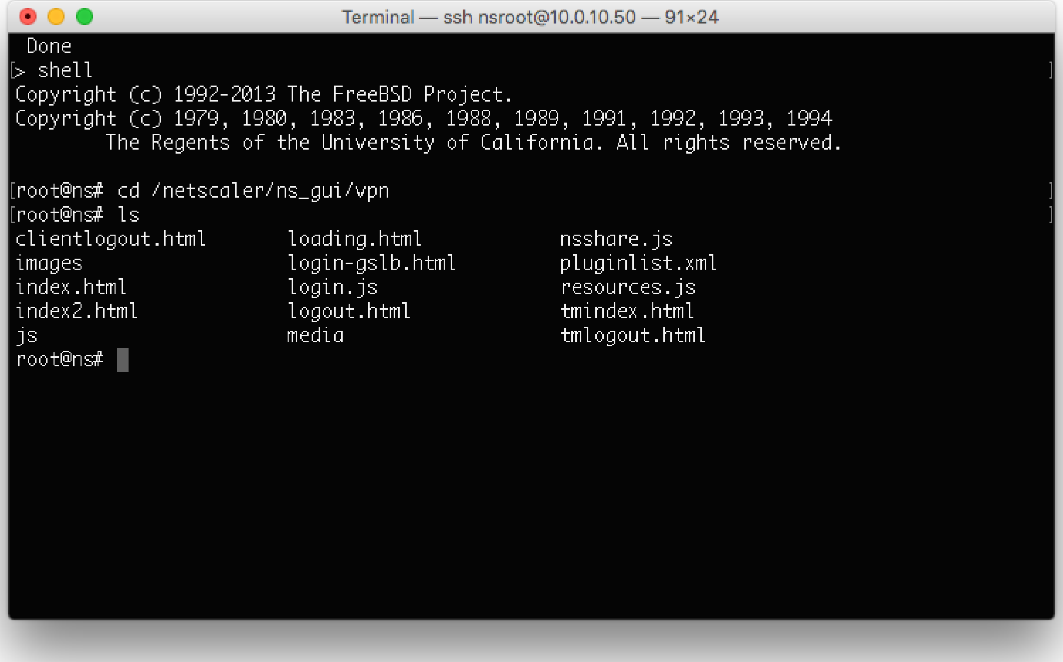
15. Connect to your Citrix NetScaler over SSH:
16. Run command: `shell`



```
 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#
```

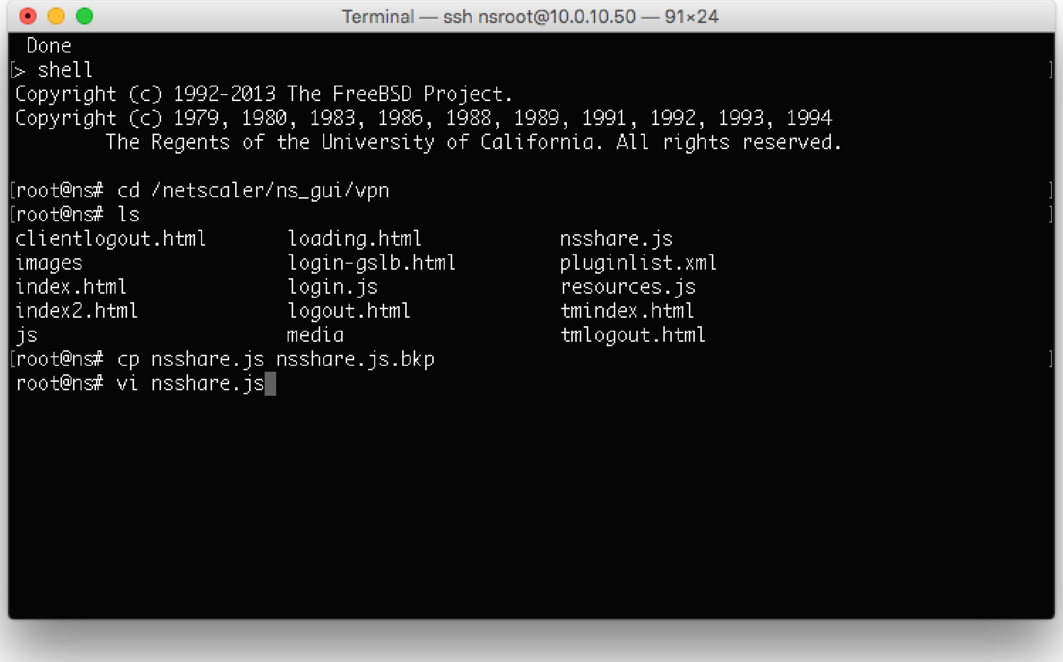
17. Run command: `cd /netscaler/ns_gui/vpn`



```
 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#
```

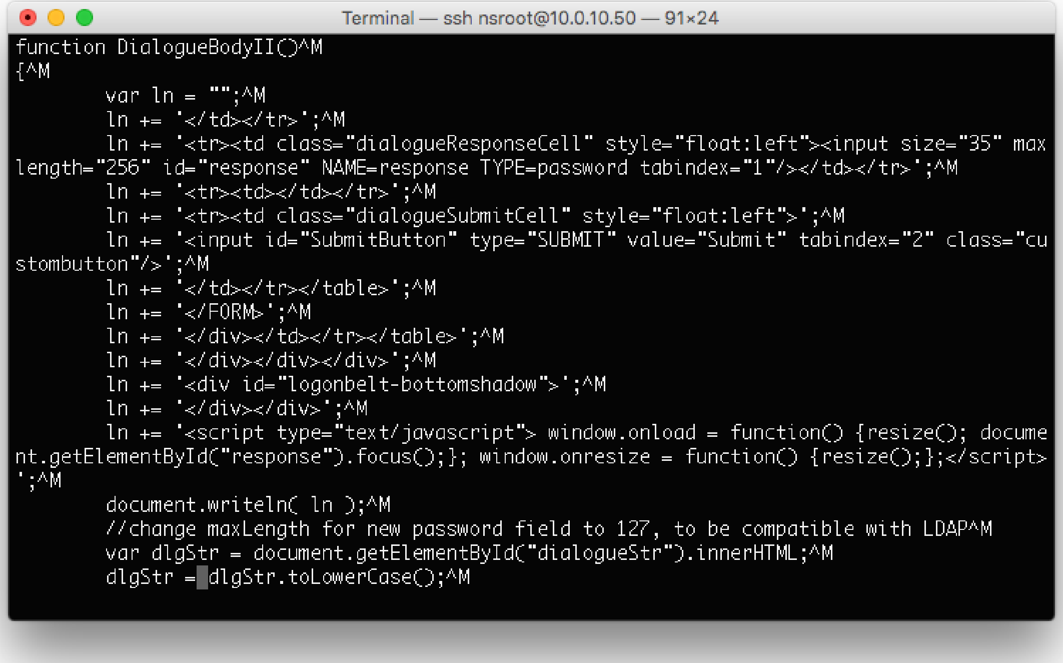
18. Create a backup of `nsshare.js` file: `cp nsshare.js nsshare.js.bkp`
19. Open file `nsshare.js` for editing: `vi nsshare.js`



```
 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
```

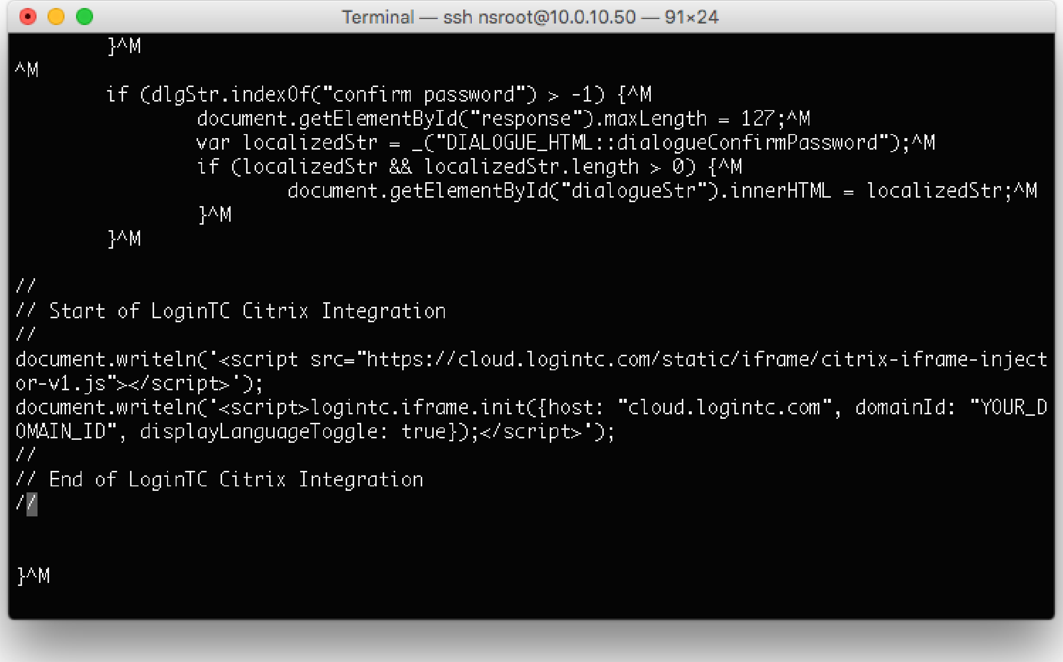
20. Scroll down to the `DialogueBodyII()` function:



```
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
```

21. Scroll down to the bottom of the `DialogueBodyII()` function and insert the Citrix Integration snippet:

```
  document.writeln('<script src="https://cloud.logintc.com/static/iframe/citrix-iframe-injector-v1.js"></script>');
  document.writeln('<script>logintc.iframe.init({host: "cloud.logintc.com", domainId: "YOUR_DOMAIN_ID", displayLanguageToggle: true});</script>');
```



```
        }^M
^M
        if (dlgStr.indexOf("confirm password") > -1) {^M
                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
//
document.writeln('<script src="https://cloud.logintc.com/static/iframe/citrix-iframe-inject
or-v1.js"></script>');
document.writeln('<script>logintc.iframe.init({host: "cloud.logintc.com", domainId: "YOUR_D
OMAIN_ID", displayLanguageToggle: true});</script>');
//
// End of LoginTC Citrix Integration
//


}^M
```

Ensure that you have entered your `domainId` in the Citrix Integration snippet

22. 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.

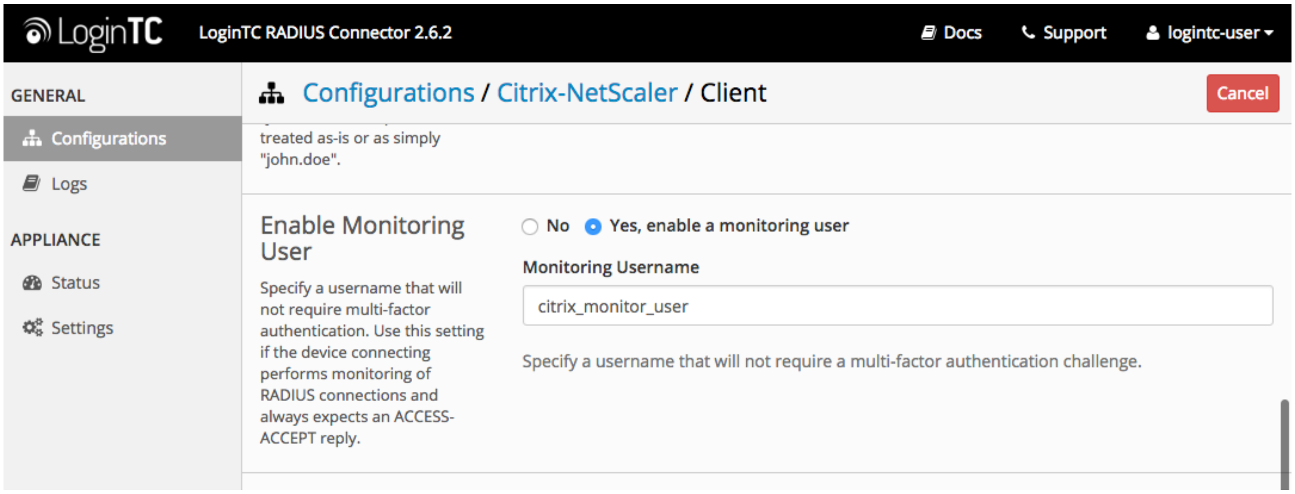
Testing

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**



treated as-is or as simply "john.doe".

Enable Monitoring User

Specify a username that will not require multi-factor 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

Monitoring Username: citrix_monitor_user

Specify a username that will not require a multi-factor authentication challenge.

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 domain dedicated for monitoring

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

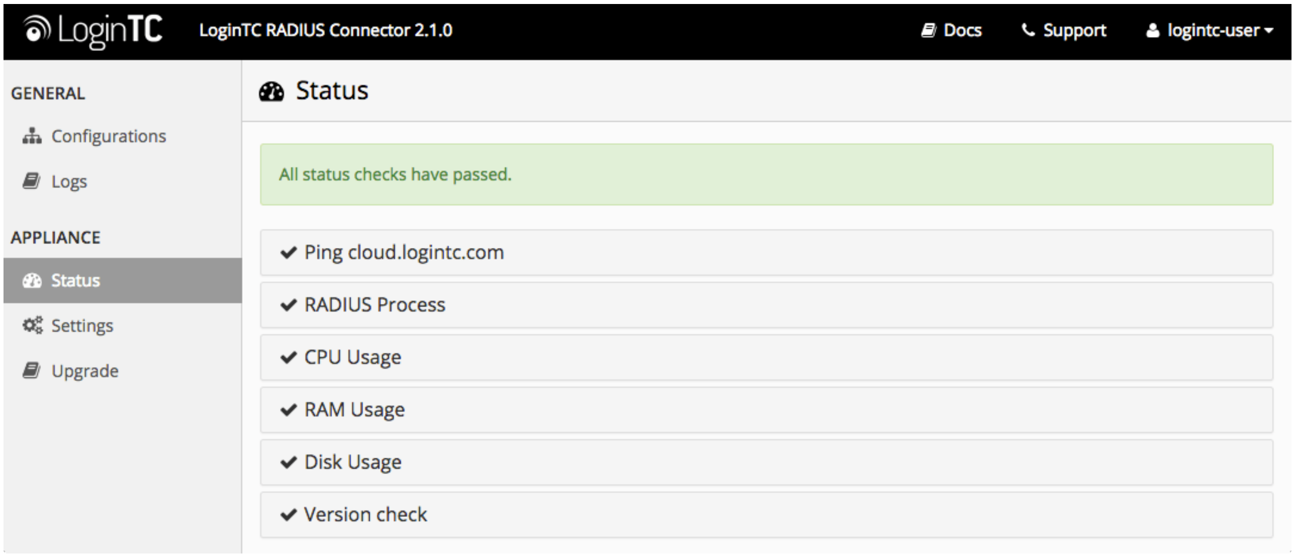
(Optional) Active Directory check for monitoring user

Recommend leveraging a dedicated service account for First Factor authentication.

Troubleshooting

Not Authenticating

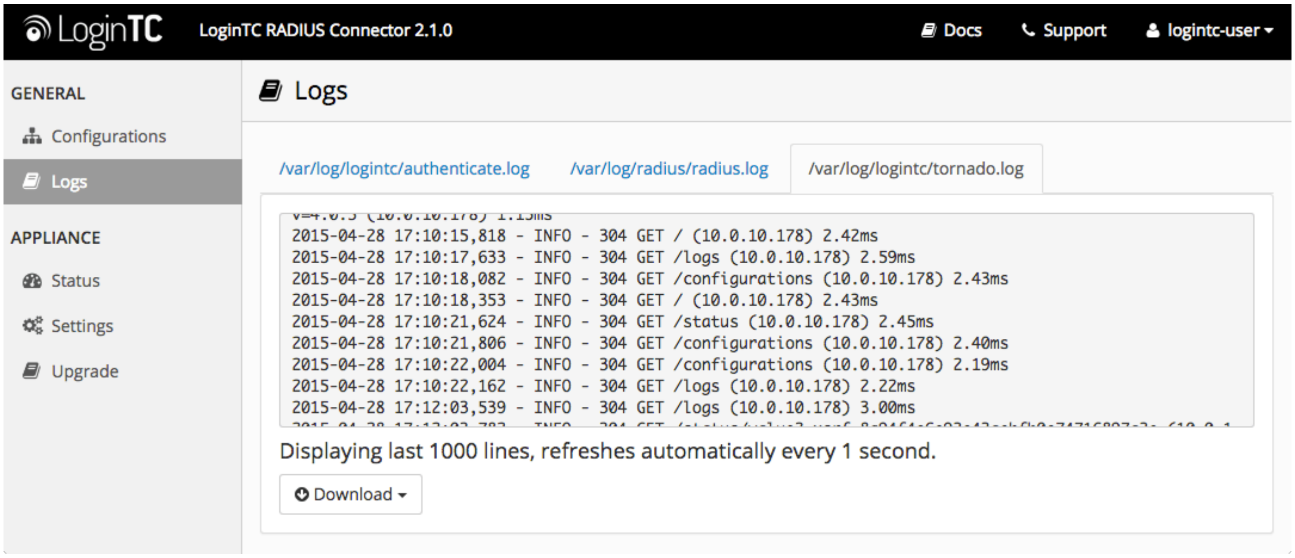
If you are unable to authenticate, navigate to your appliance **web interface** URL and click **Status**:



All status checks have passed.

- ✓ Ping cloud.logintc.com
- ✓ RADIUS Process
- ✓ CPU Usage
- ✓ RAM Usage
- ✓ Disk Usage
- ✓ Version check

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


LoginTC
LoginTC RADIUS Connector 2.1.0
Docs
Support
logintc-user
GENERAL
Configurations
Logs
APPLIANCE
Status
Settings
Upgrade
Logs
/var/log/logintc/authenticate.log
/var/log/radius/radius.log
/var/log/logintc/tornado.log

```
v=4.0.3 (10.0.10.178) 1.13ms
2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms
2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms
2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms
2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms
2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms
2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms
2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms
2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms
```

Displaying last 1000 lines, refreshes automatically every 1 second.

Email Support

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