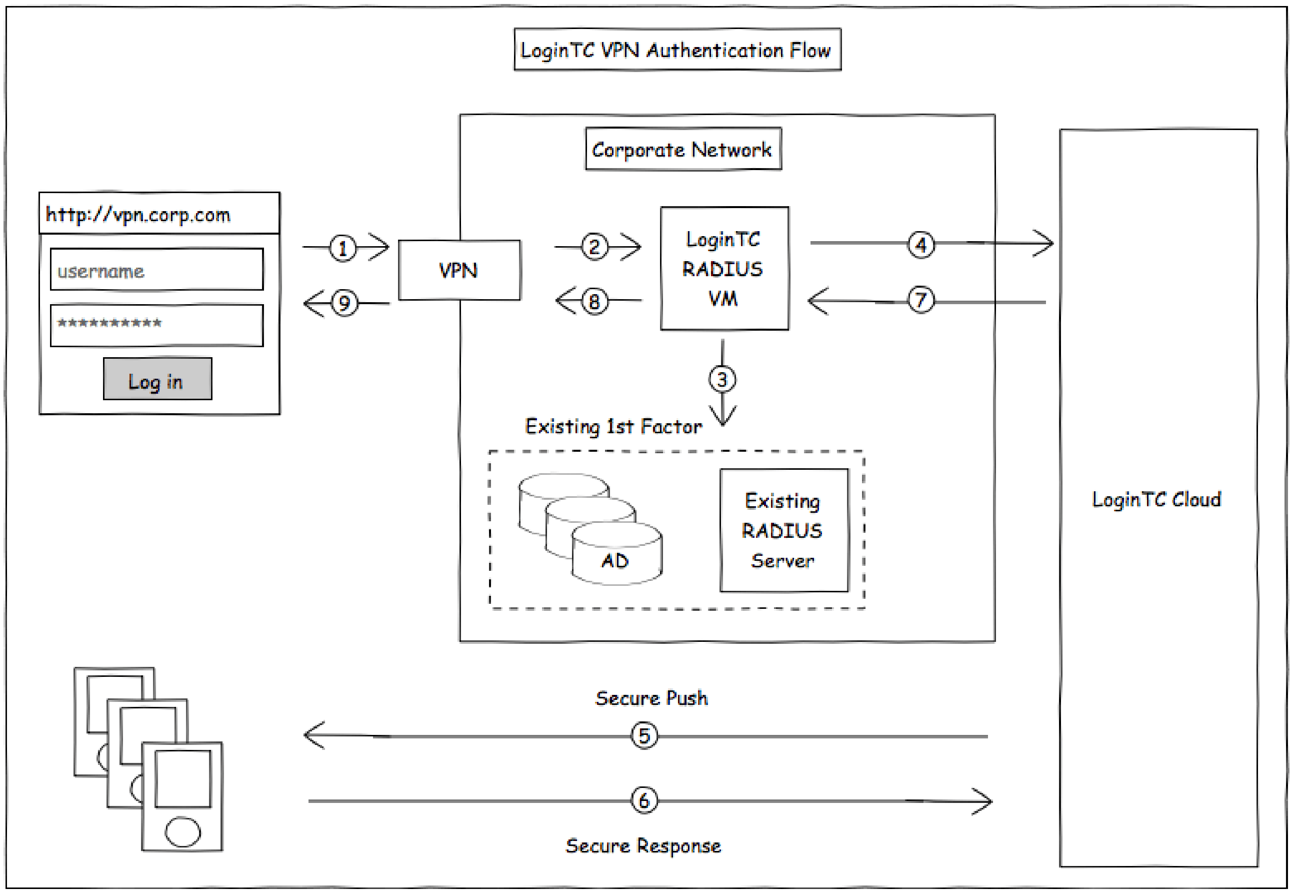
Two factor authentication for OpenVPN Access Server

logintc.com/docs/connectors/openvpn-as.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 OpenVPN Access Server to use LoginTC for the most secure two-factor authentication.



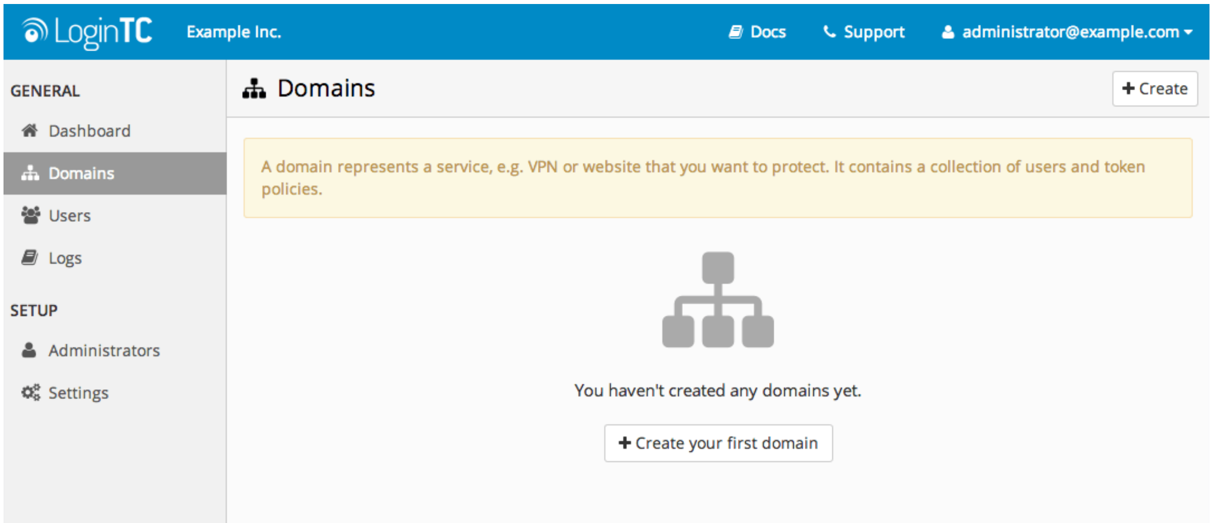
Prerequisites

Before proceeding, please ensure you have the following:

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.

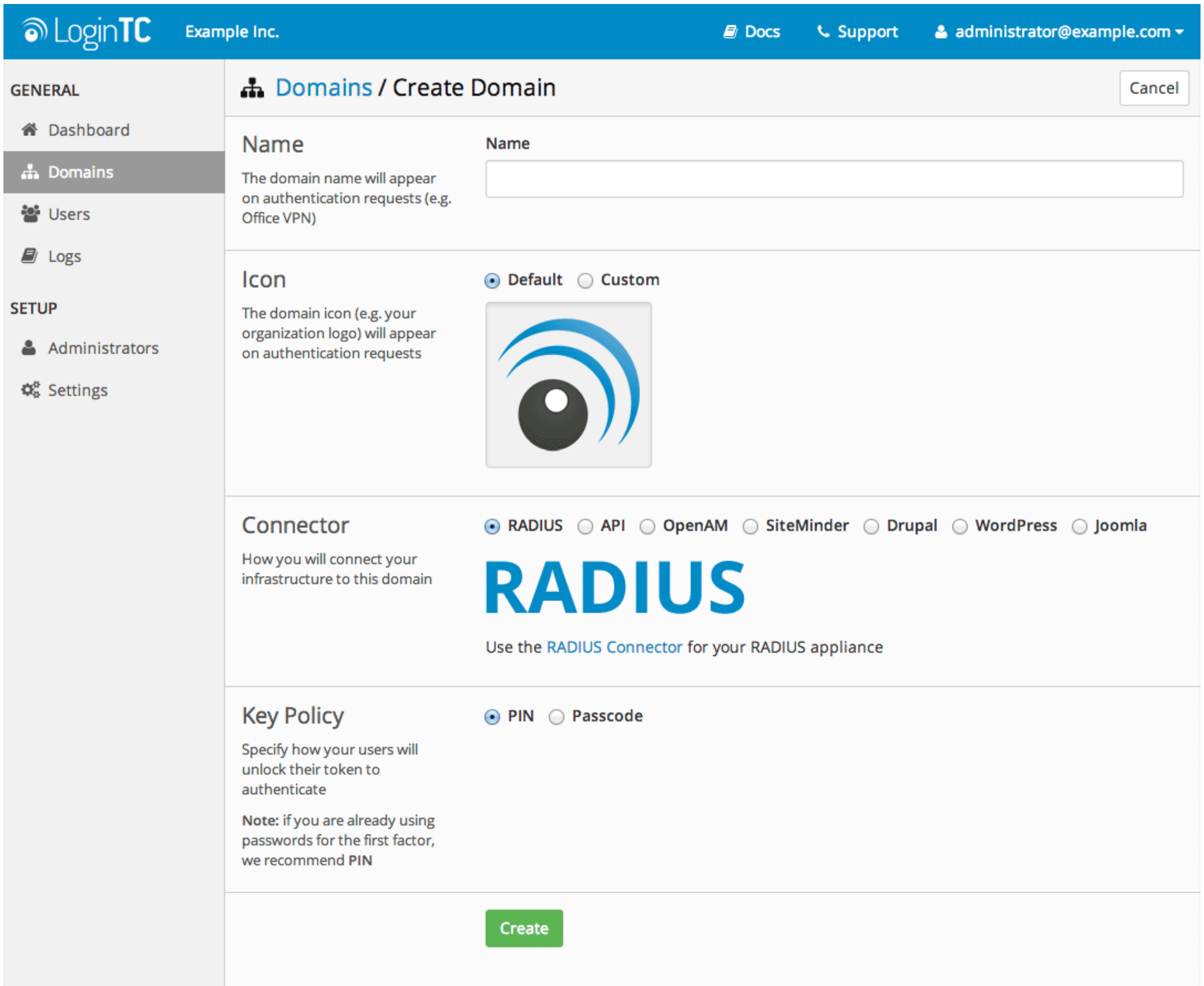
1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Add Domain**:



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:



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

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

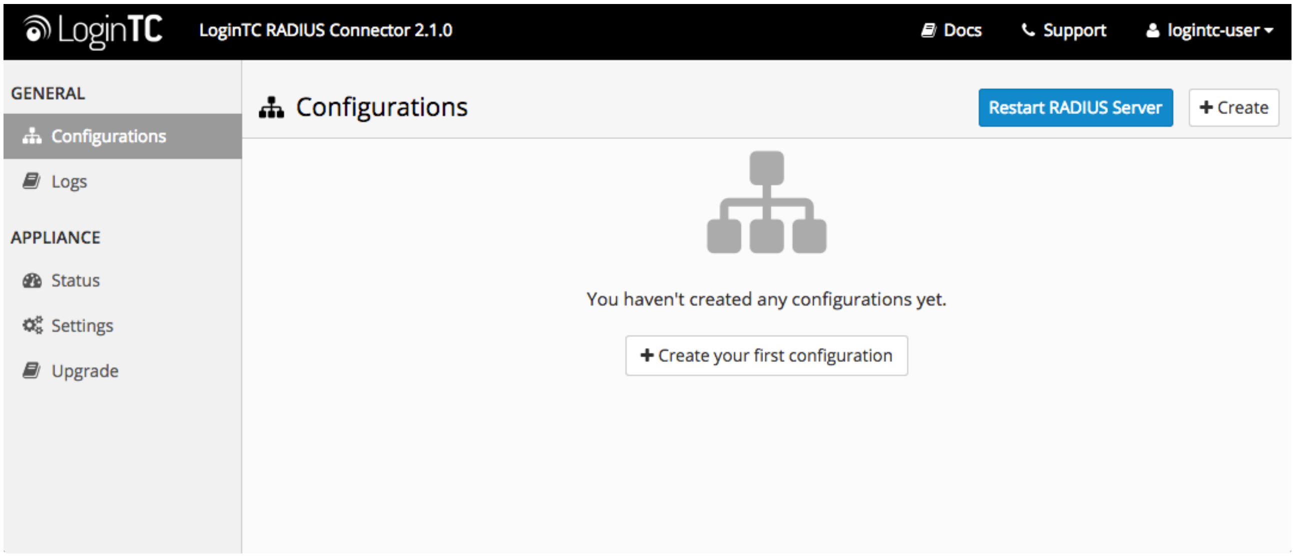
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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.

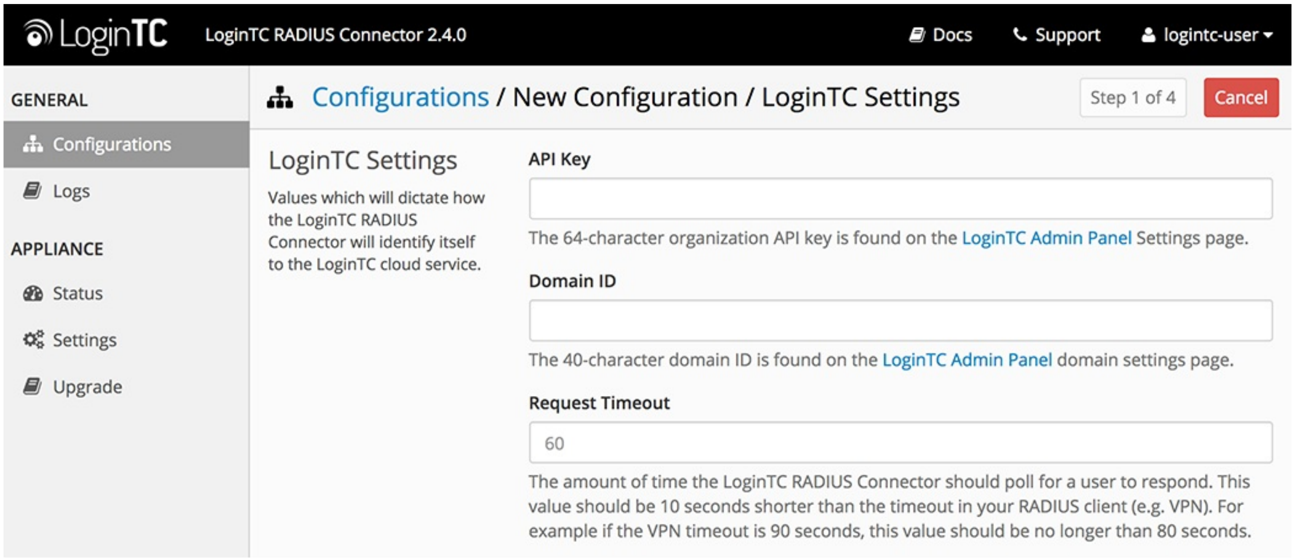
Create a new configuration file by clicking **+ Create your first configuration**:



You haven't created any configurations yet.

LoginTC Settings

Configure which LoginTC organization and domain to use:



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

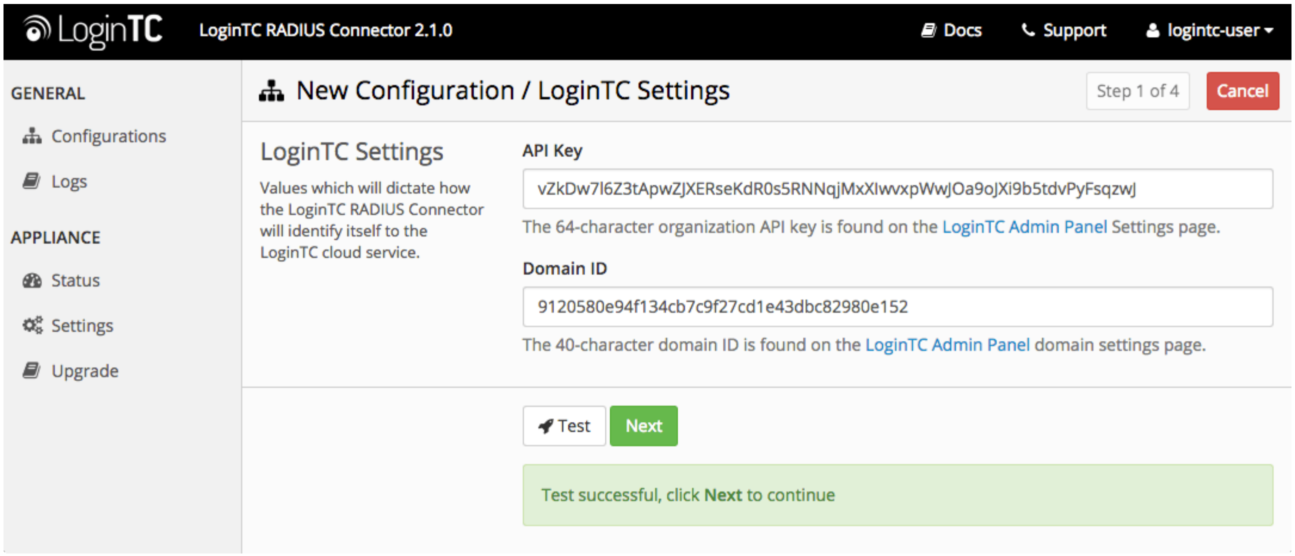
The amount of time the LoginTC RADIUS Connector should poll for a user to respond. This value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

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**:



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

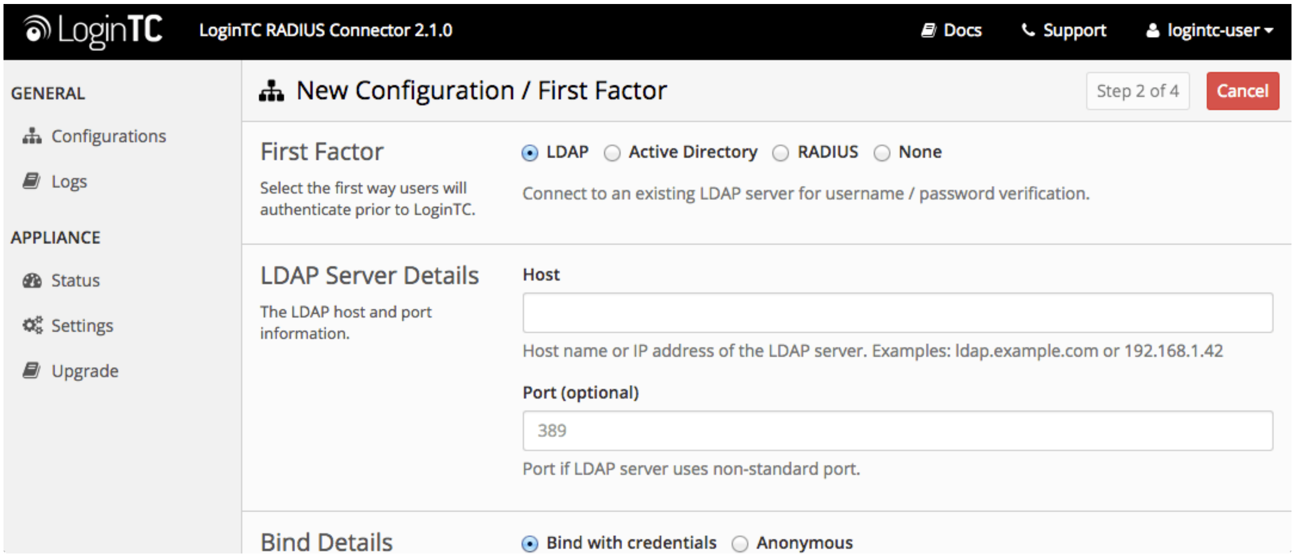
9120580e94f134cb7c9f27cd1e43dbc82980e152

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

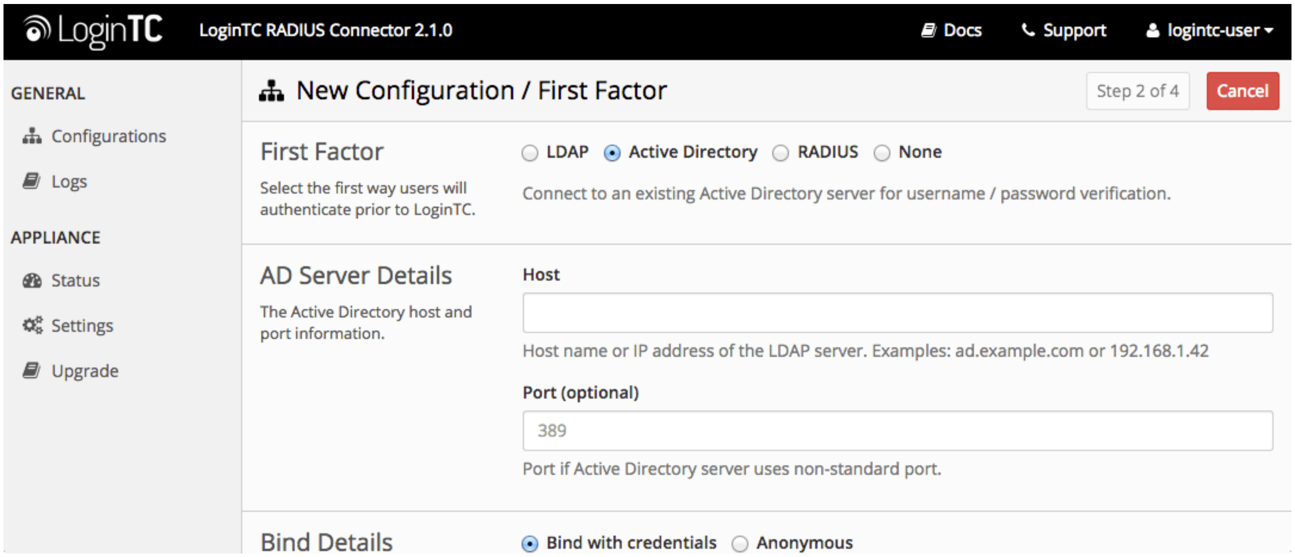
Port if LDAP server uses non-standard port.

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:

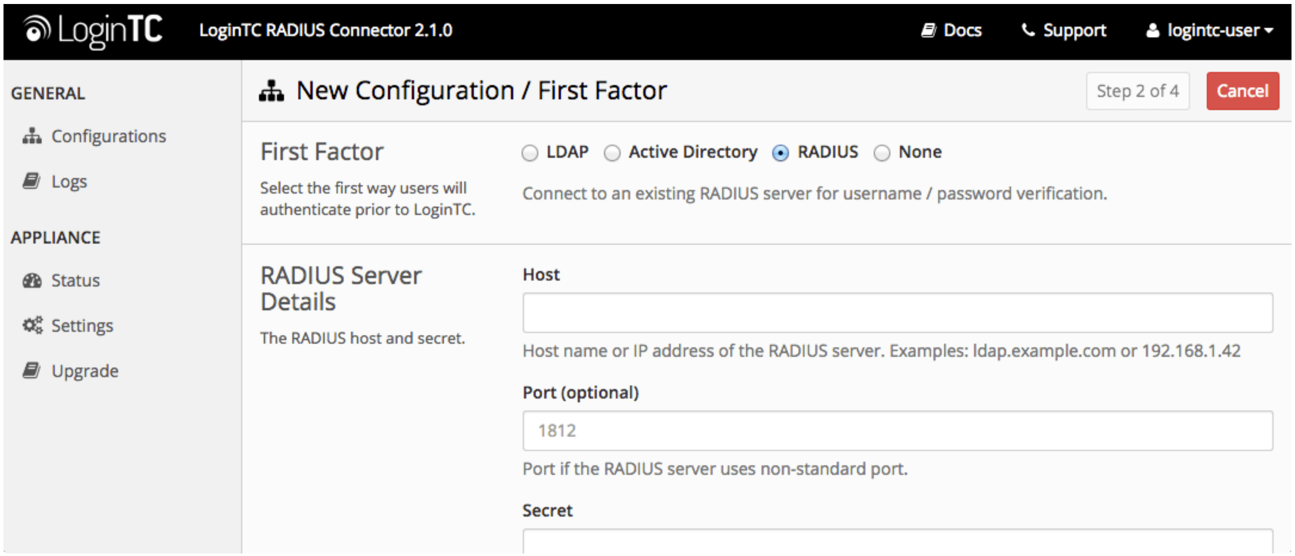
Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The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

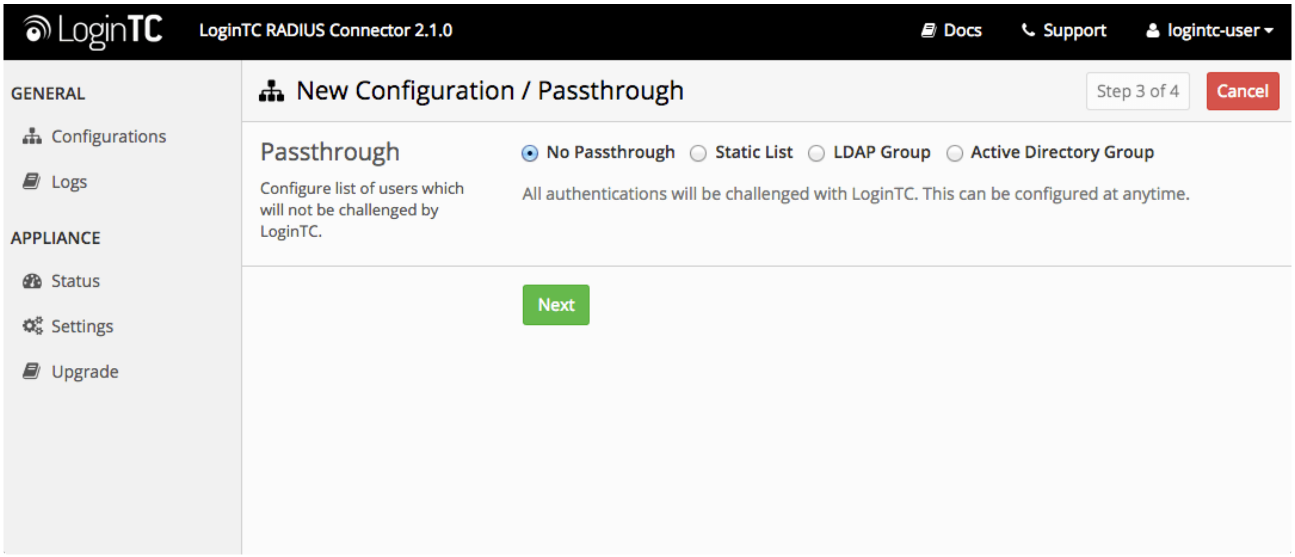
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.



Passthrough

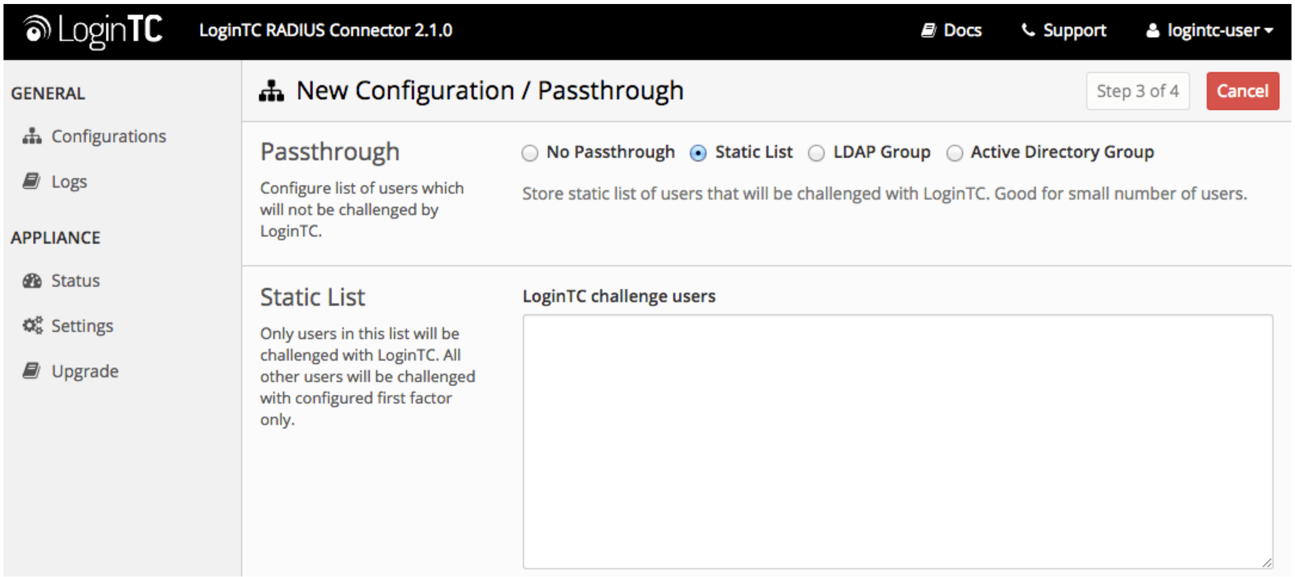
Configure list of users which will not be challenged by LoginTC.

● 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.

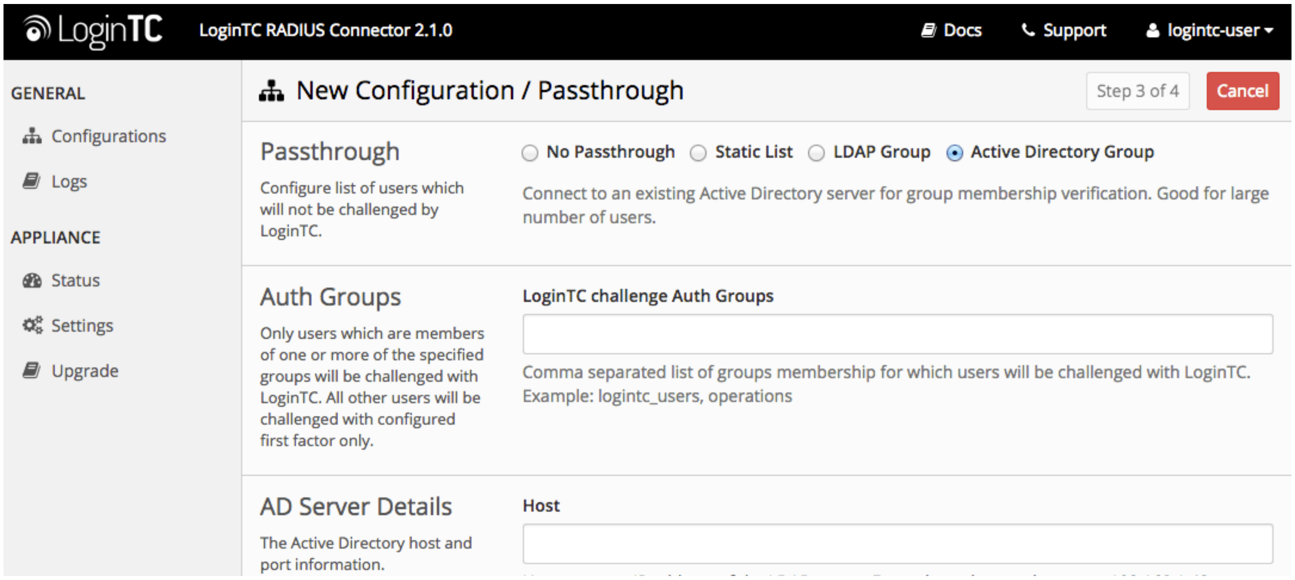
LoginTC challenge users

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`

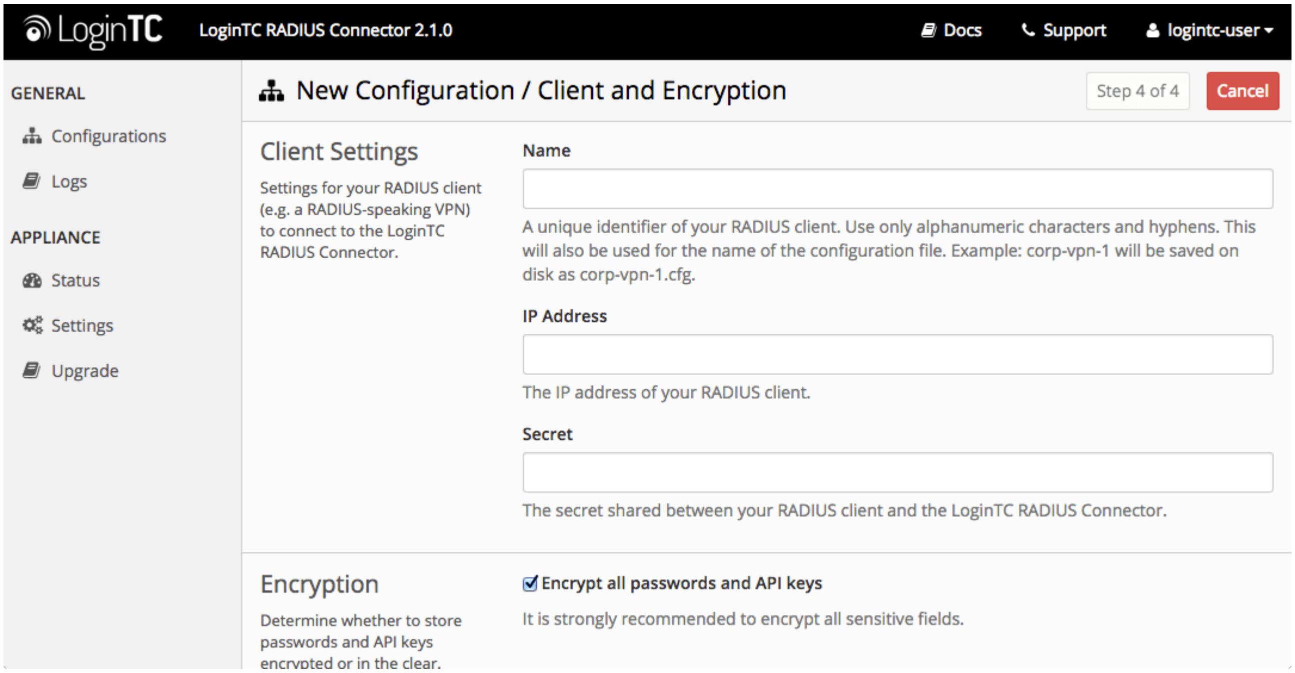
Configuration Simplified

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 RADIUS-speaking VPN):



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.

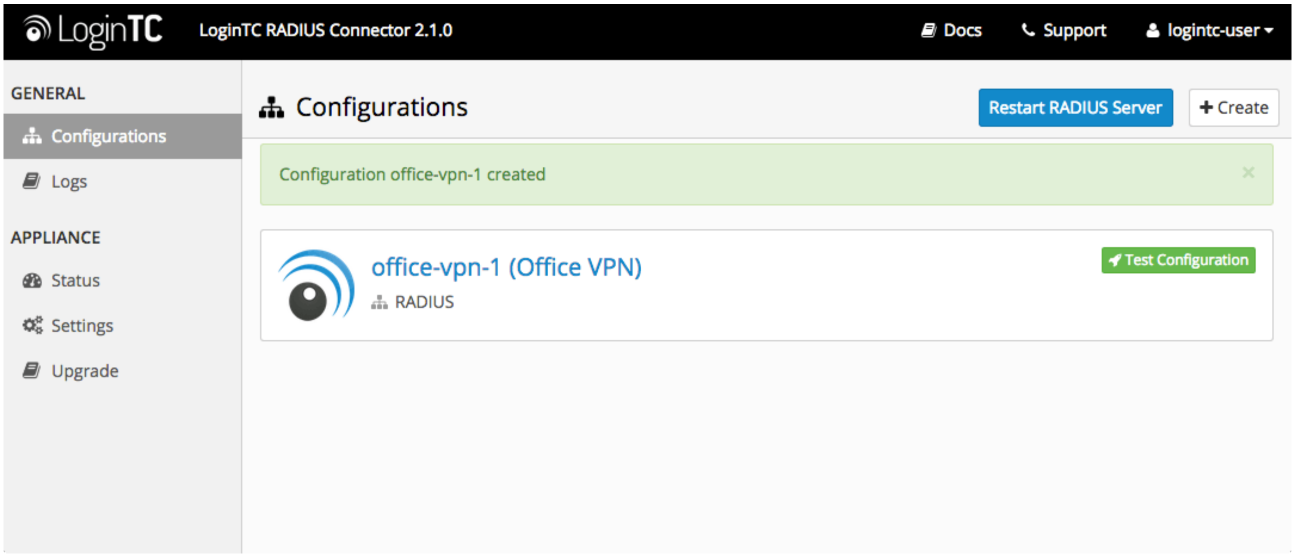
Client configuration values:

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`

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

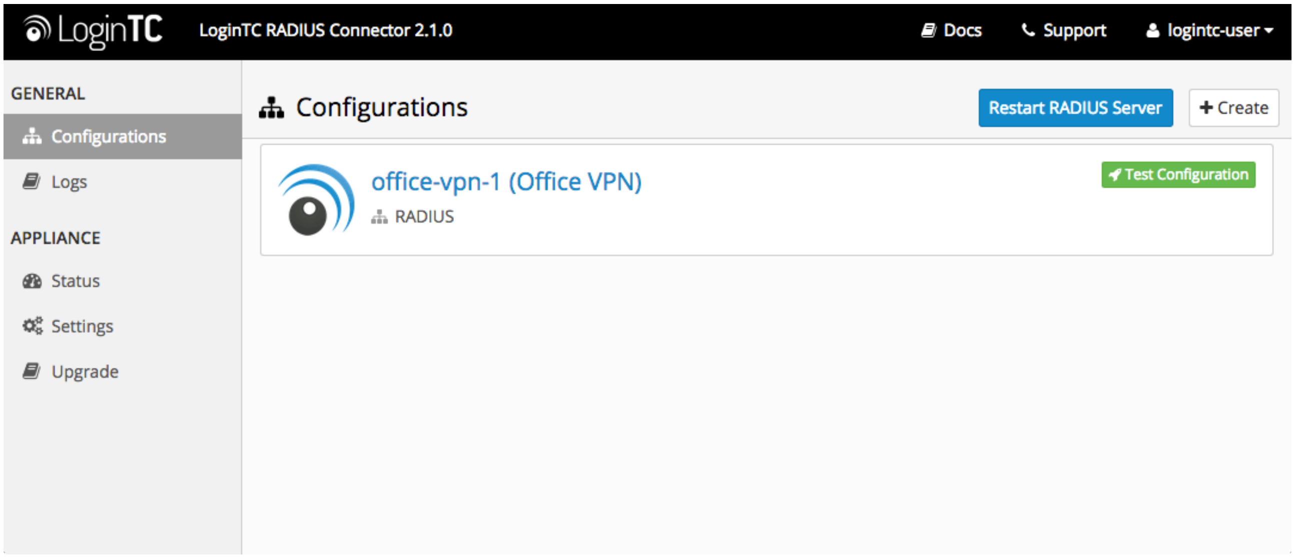
office-vpn-1 (Office VPN)

RADIUS

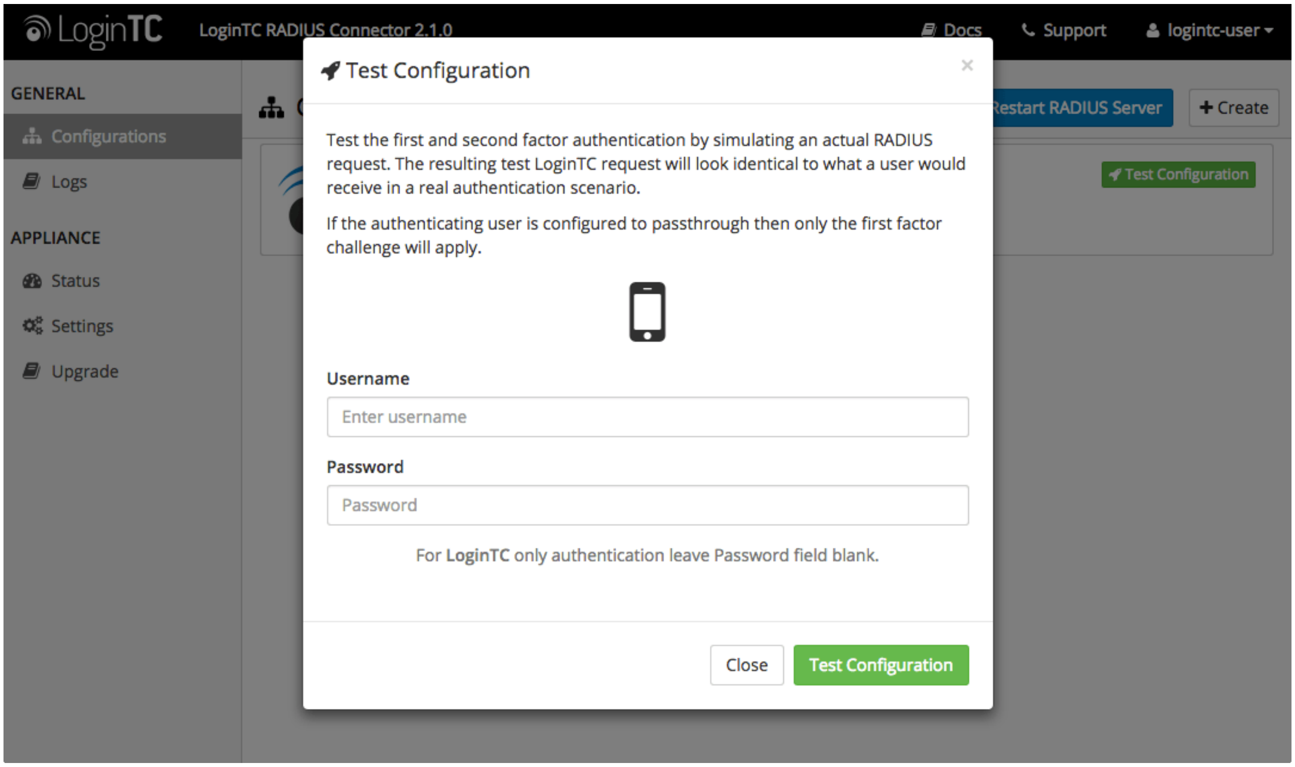
Testing

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 applianceweb **interface** URL:



Click **Test Configuration**:



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.

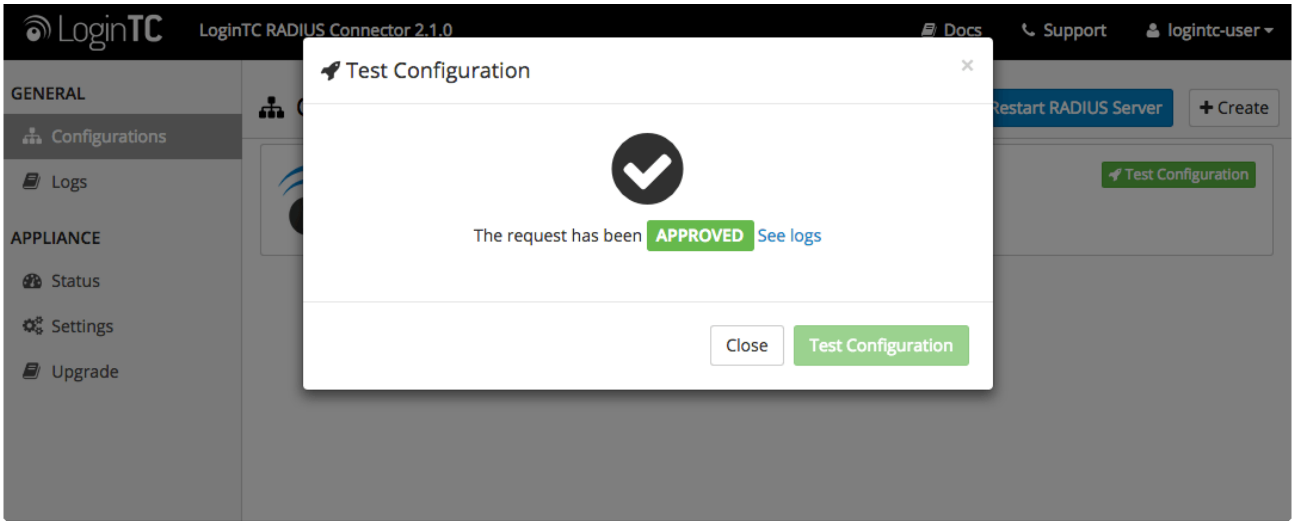
If the authenticating user is configured to passthrough then only the first factor challenge will apply.

Username: Enter username

Password: Password

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:

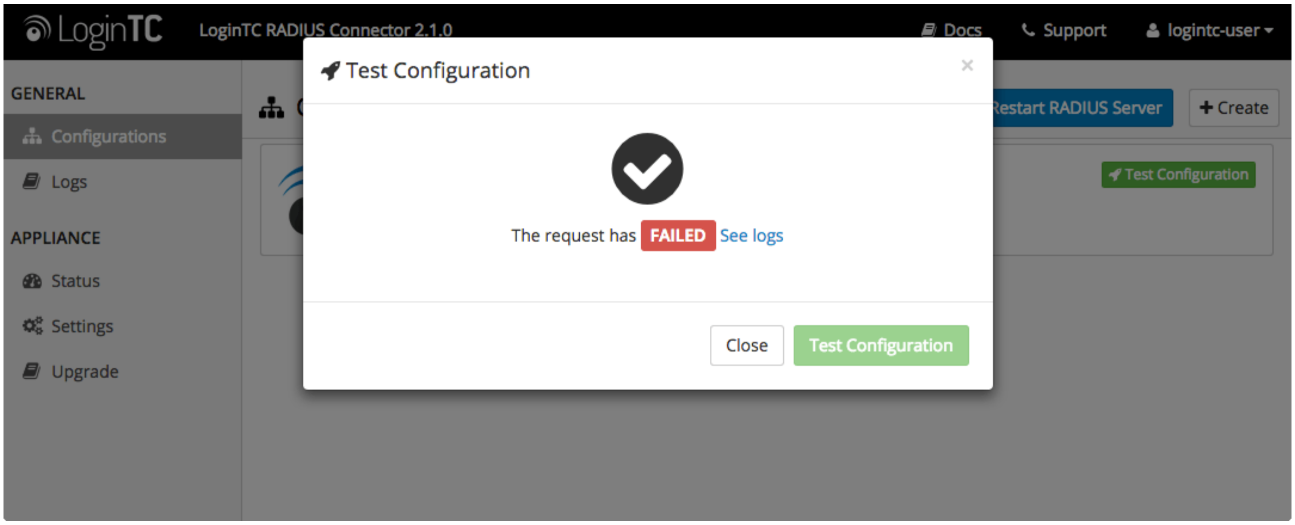


Test Configuration

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!

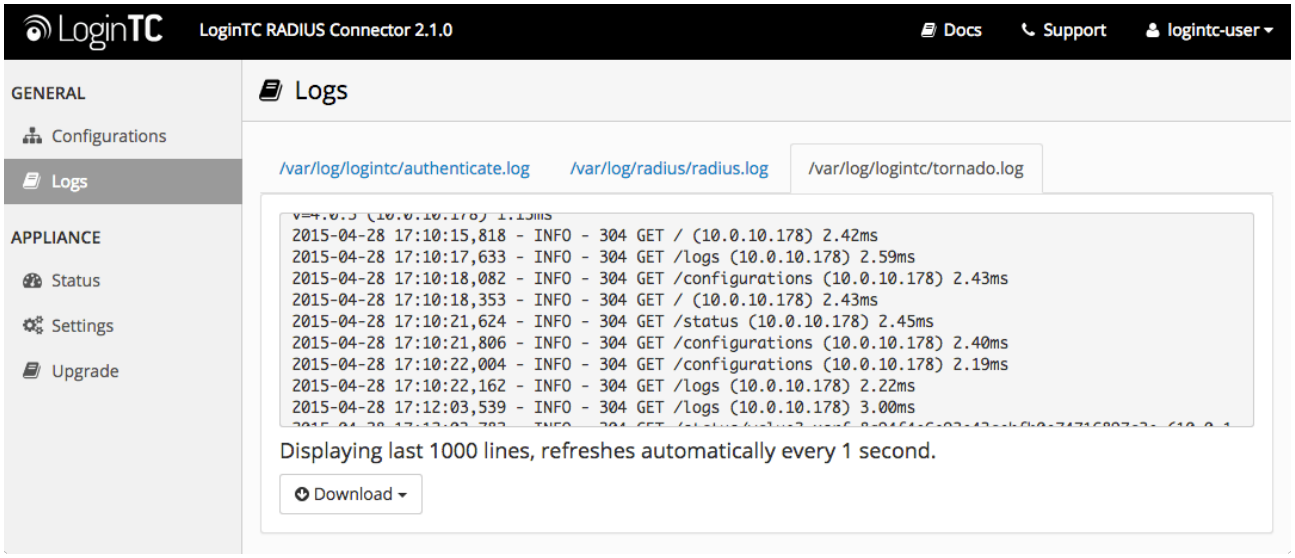
If there was an error during testing, the following will appear:



Test Configuration

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

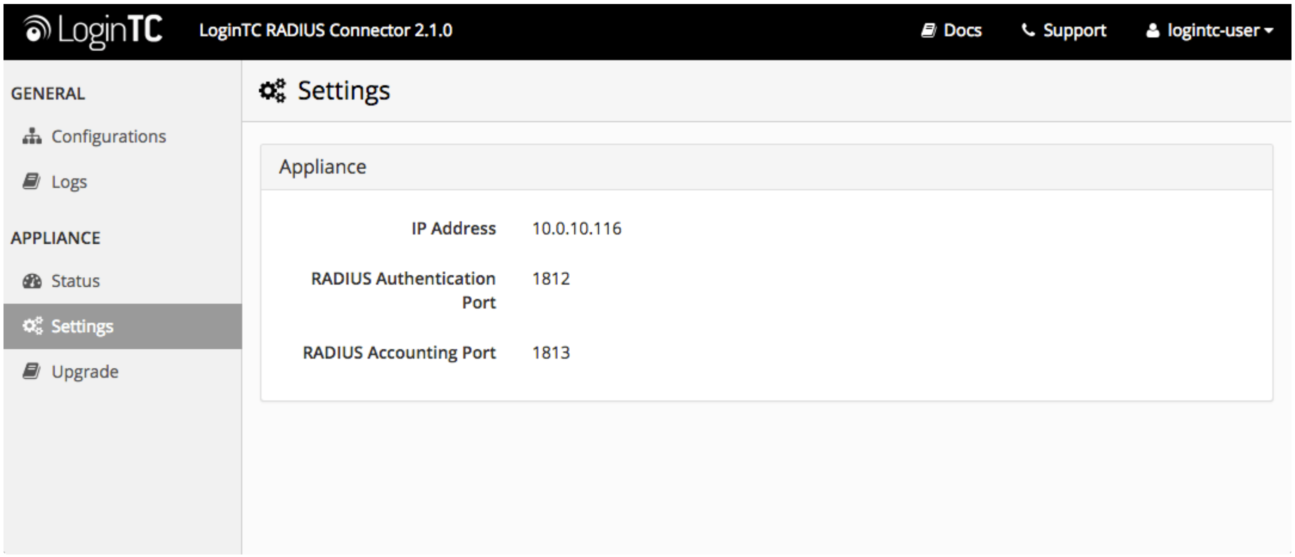
```
v=4.0.5 (10.0.10.178) 1.15ms
2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms
2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms
2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms
2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
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.

OpenVPN AS Quick Config Guide

Once you are satisfied with your setup, configure your OpenVPN Access Server to use the LoginTC RADIUS Connector.

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



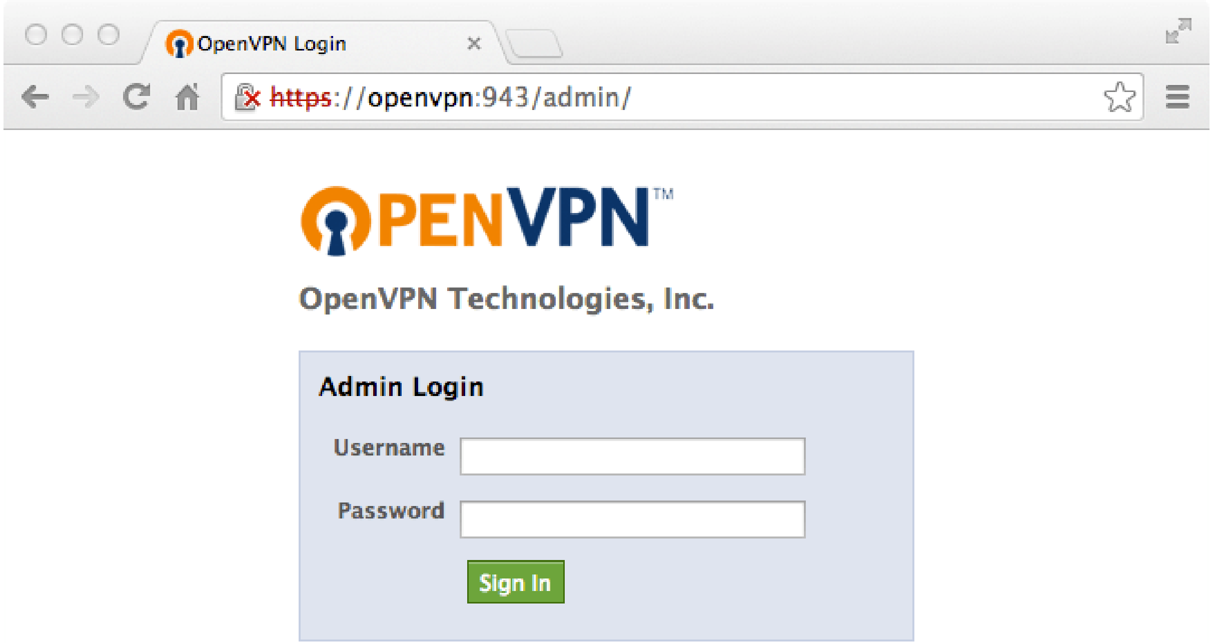
Settings

Appliance

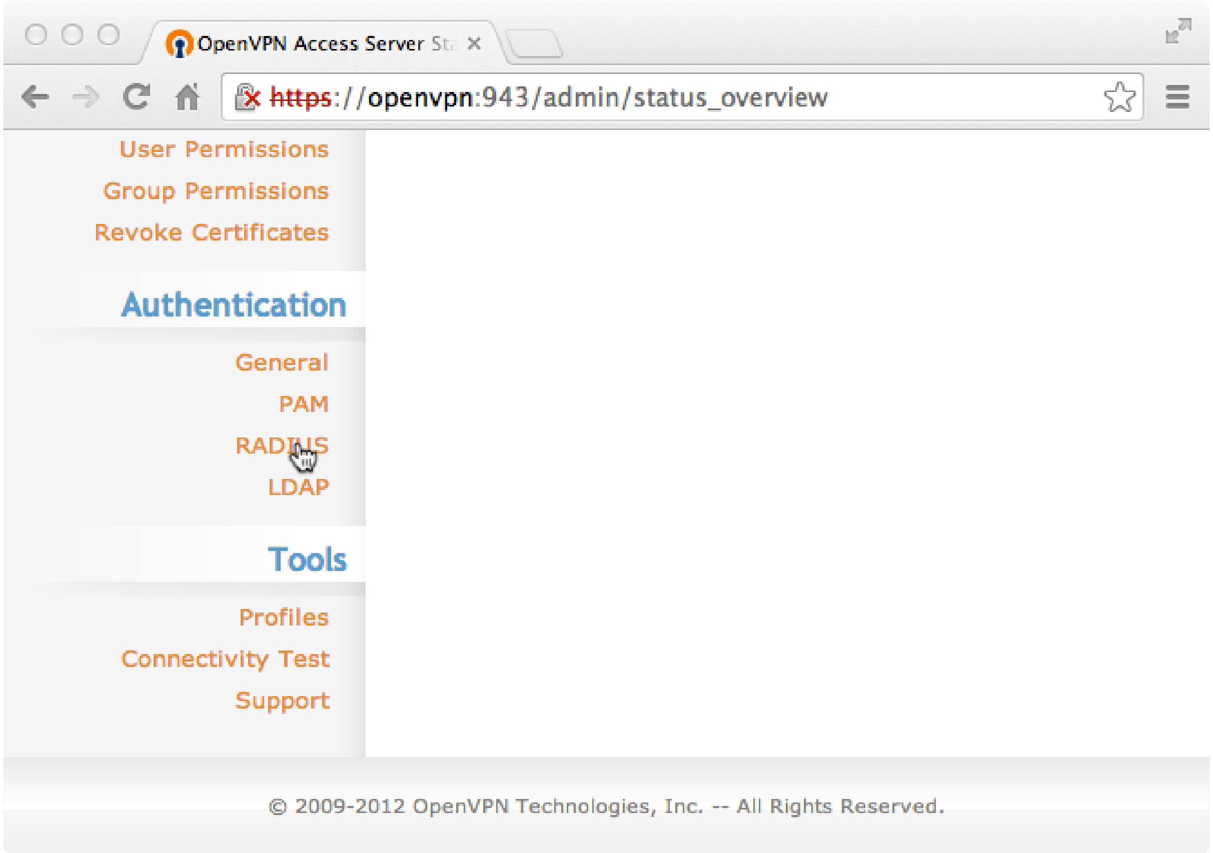
IP Address	10.0.10.116
RADIUS Authentication Port	1812
RADIUS Accounting Port	1813

The following are quick steps to get VPN access protected with LoginTC. The instructions can be used for existing setups as well.

1. Sign In to your OpenVPN Access Server

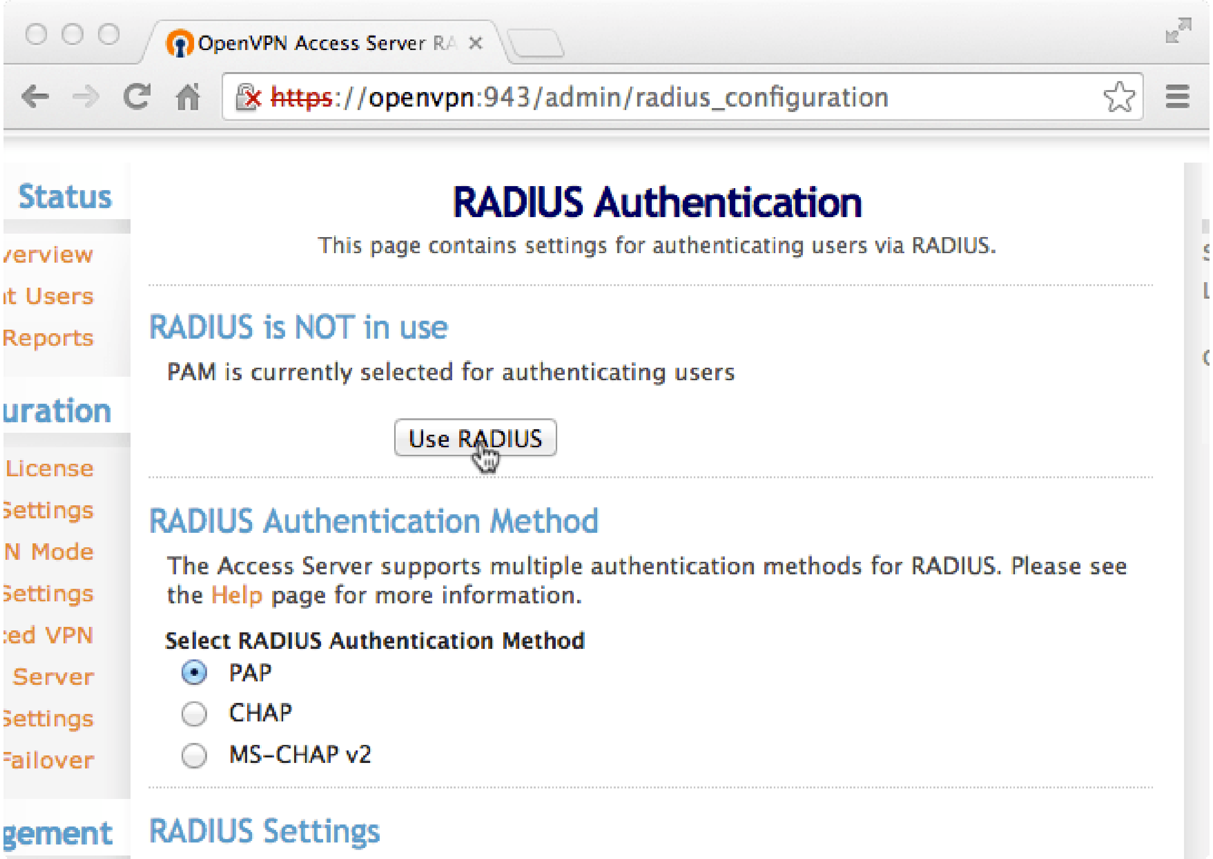


2. Under **Authentication** click **RADIUS**:



© 2009-2012 OpenVPN Technologies, Inc. -- All Rights Reserved.

3. If "RADIUS is NOT in use" is present, click **Use RADIUS** button:



RADIUS Authentication

This page contains settings for authenticating users via RADIUS.

RADIUS is NOT in use

PAM is currently selected for authenticating users

RADIUS Authentication Method

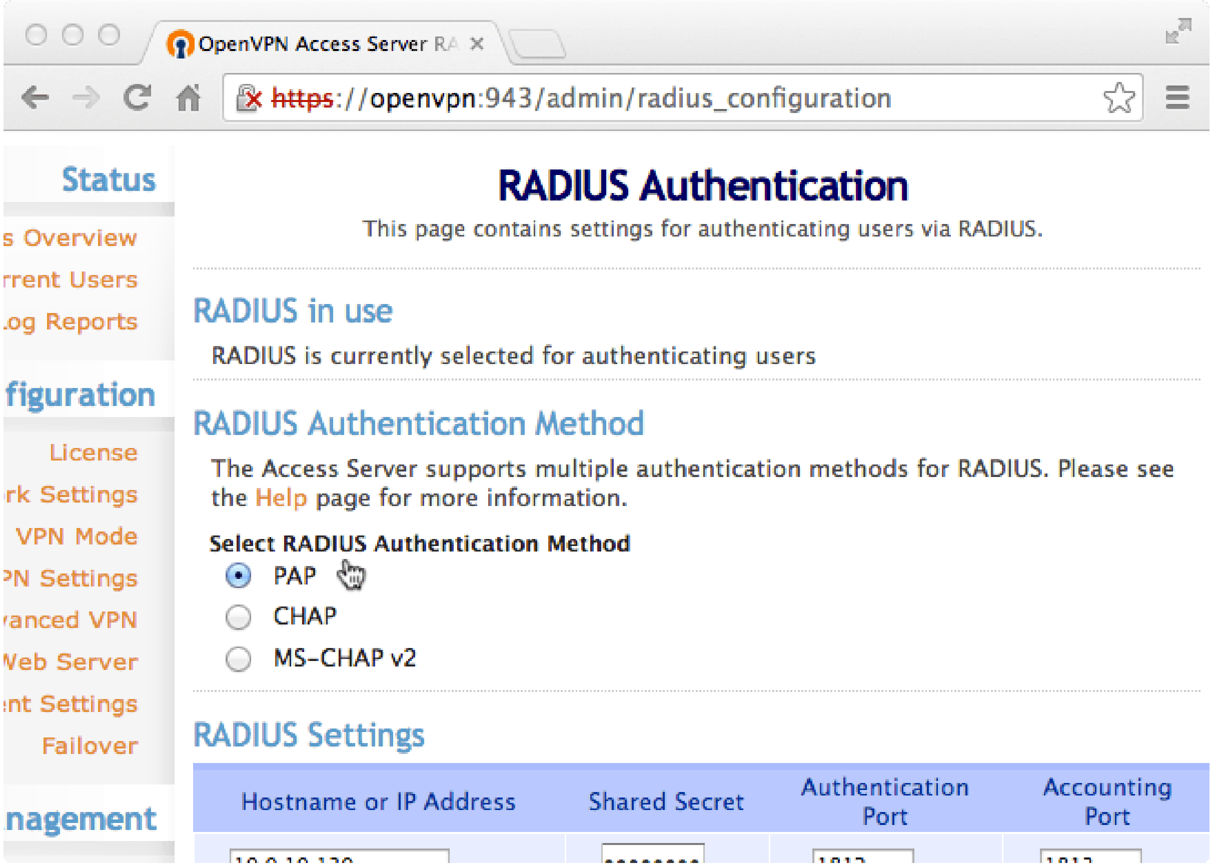
The Access Server supports multiple authentication methods for RADIUS. Please see the Help page for more information.

Select RADIUS Authentication Method

● PAP
○ CHAP
○ MS-CHAP v2

RADIUS Settings

4. Under "RADIUS Authentication Method" select **PAP**:



https://openvpn:943/admin/radius_configuration

RADIUS Authentication

This page contains settings for authenticating users via RADIUS.

RADIUS in use

RADIUS is currently selected for authenticating users

RADIUS Authentication Method

The Access Server supports multiple authentication methods for RADIUS. Please see the Help page for more information.

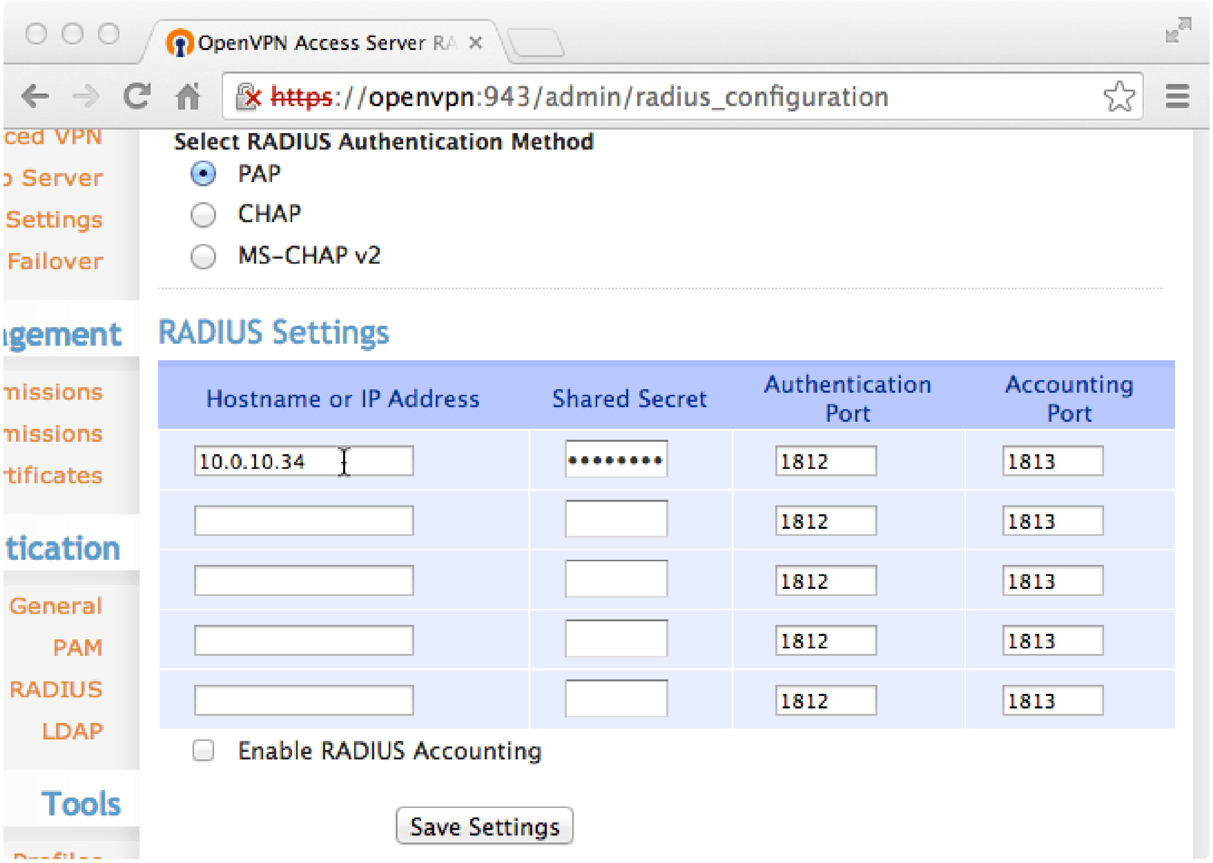
Select RADIUS Authentication Method

● PAP
○ CHAP
○ MS-CHAP v2

RADIUS Settings

Hostname or IP Address	Shared Secret	Authentication Port	Accounting Port

5. Under "RADIUS Settings" add a new entry to the form:



https://openvpn:943/admin/radius_configuration

Select RADIUS Authentication Method

● PAP
○ CHAP
○ MS-CHAP v2

RADIUS Settings

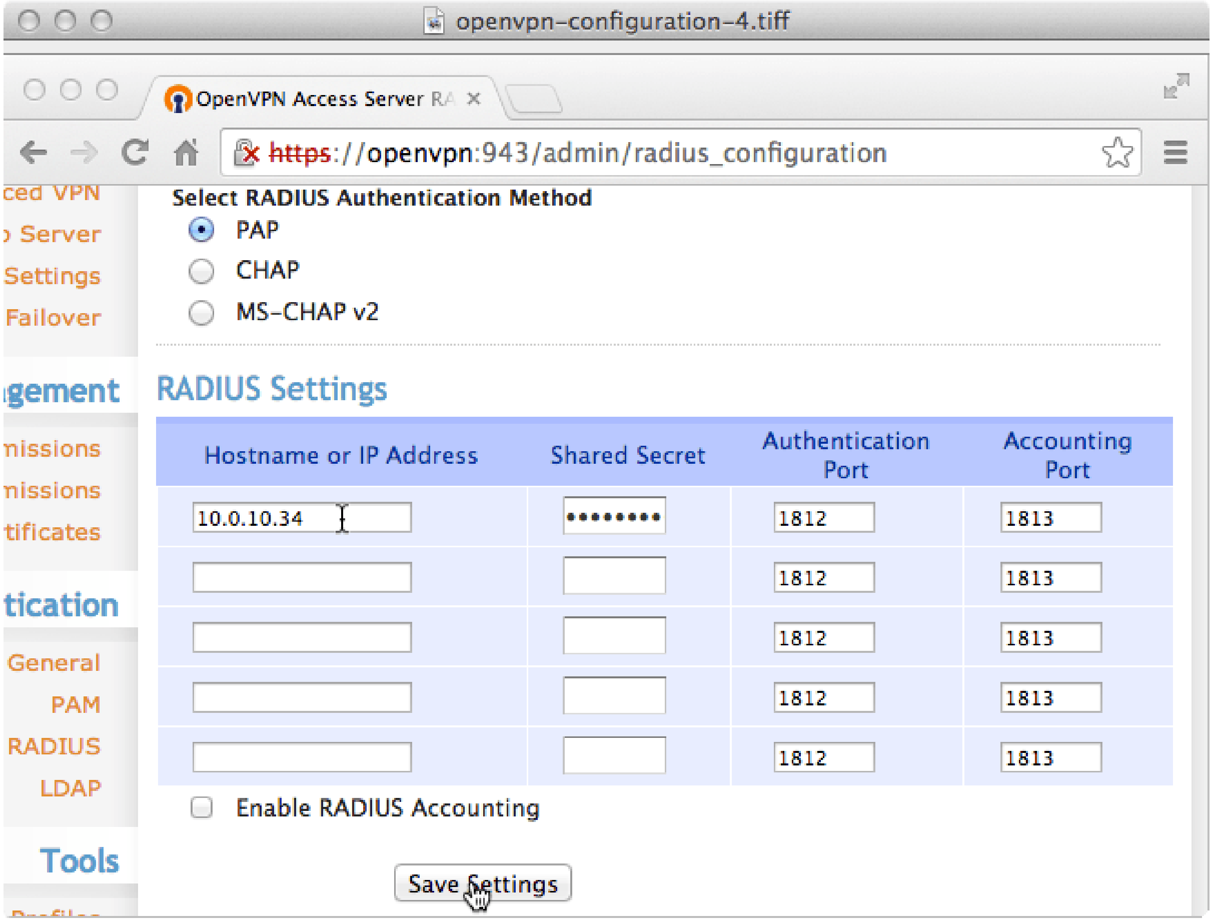
Hostname or IP Address	Shared Secret	Authentication Port	Accounting Port
10.0.10.34	••••••••	1812	1813
		1812	1813
		1812	1813
		1812	1813
		1812	1813

□ Enable RADIUS Accounting

Save Settings

Property	Explanation	Example
`Hostname or IP Address`	Address of LoginTC RADIUS Connector	192.168.1.1
`Shared Secret`	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret
`Authentication Port`	RADIUS authentication port. Must be 1812.	1812
`Accounting Port`	RADIUS accounting port. Must be 1813	1813

6. Click **Save Settings**:



Select RADIUS Authentication Method

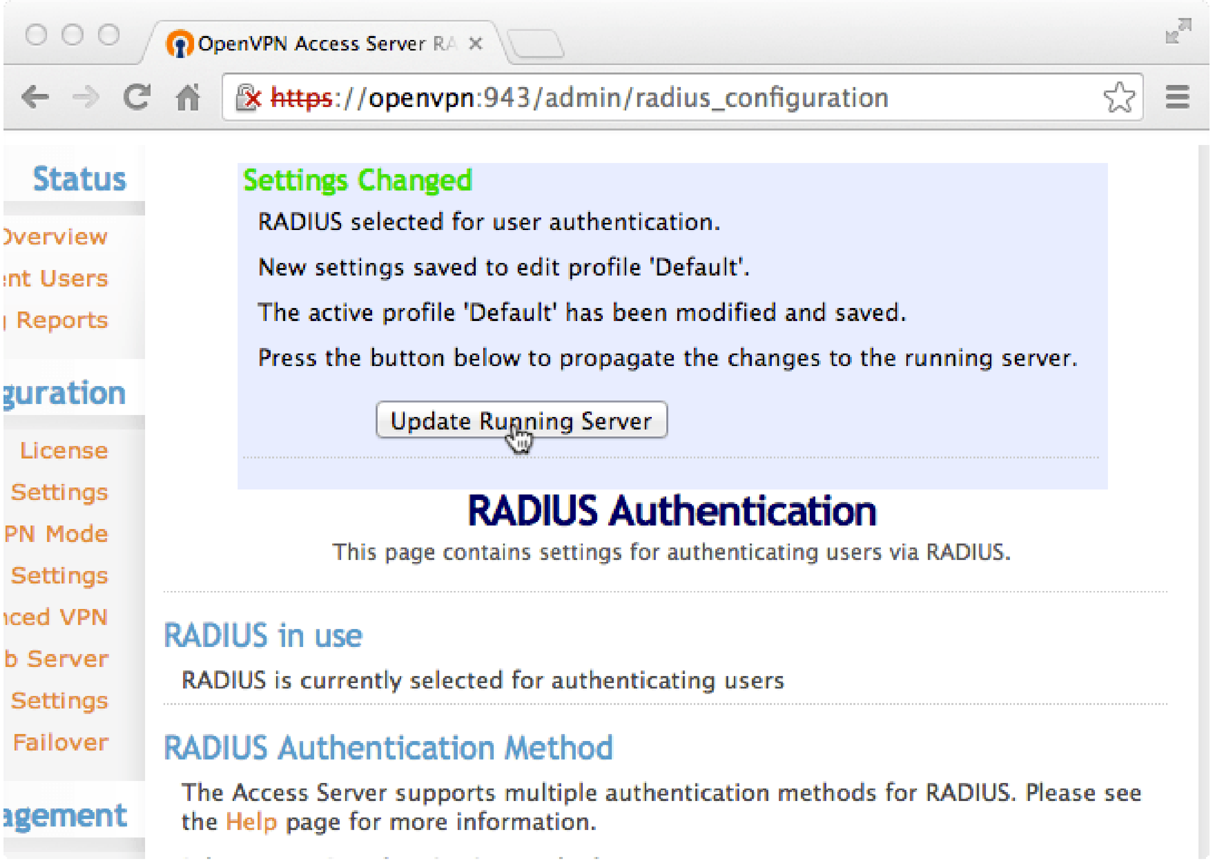
● PAP
○ CHAP
○ MS-CHAP v2

RADIUS Settings

Hostname or IP Address	Shared Secret	Authentication Port	Accounting Port
10.0.10.34	•••••••••	1812	1813
		1812	1813
		1812	1813
		1812	1813
		1812	1813

☐ Enable RADIUS Accounting

7. Click **Update Running Server**:



Settings Changed

RADIUS selected for user authentication.

New settings saved to edit profile 'Default'.

The active profile 'Default' has been modified and saved.

Press the button below to propagate the changes to the running server.

RADIUS Authentication

This page contains settings for authenticating users via RADIUS.

RADIUS in use

RADIUS is currently selected for authenticating users

RADIUS Authentication Method

The Access Server supports multiple authentication methods for RADIUS. Please see the Help page for more information.

To test, navigate to your OpenVPN Access Server clientless VPN portal or use OpenVPN Connect and attempt access.

Troubleshooting

No Network Connection

1. First ensure that your LoginTC RADIUS Connector is configured to have a virtual network adapter on `eth0`
2. Ensure that the virtual network adapter MAC address matches the one in the file `/etc/sysconfig/network-scripts/ifcfg-eth0`
3. Restart the networking service:

   ```
   service network restart
   ```

4. If you notice the error that `eth0` is not enabled, then check driver messages for more information:

   ```
   dmesg | grep eth
   ```

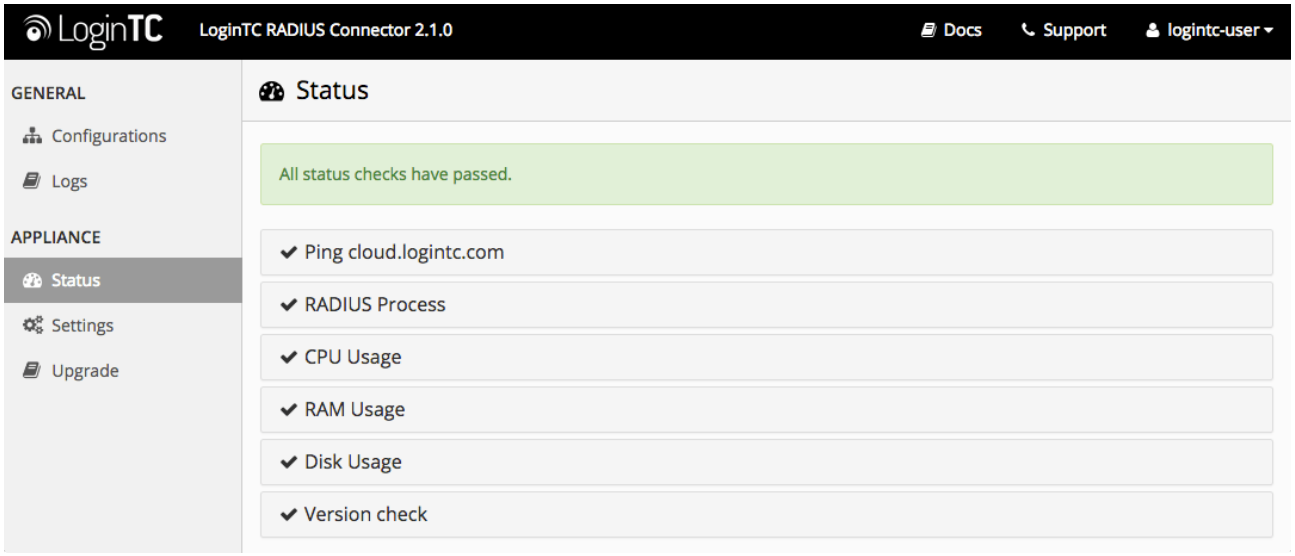
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

   ```
   mv /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth1
   ```

   Open the file and update the `DEVICE="eth0"` line to `DEVICE="eth1"`

Not Authenticating

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

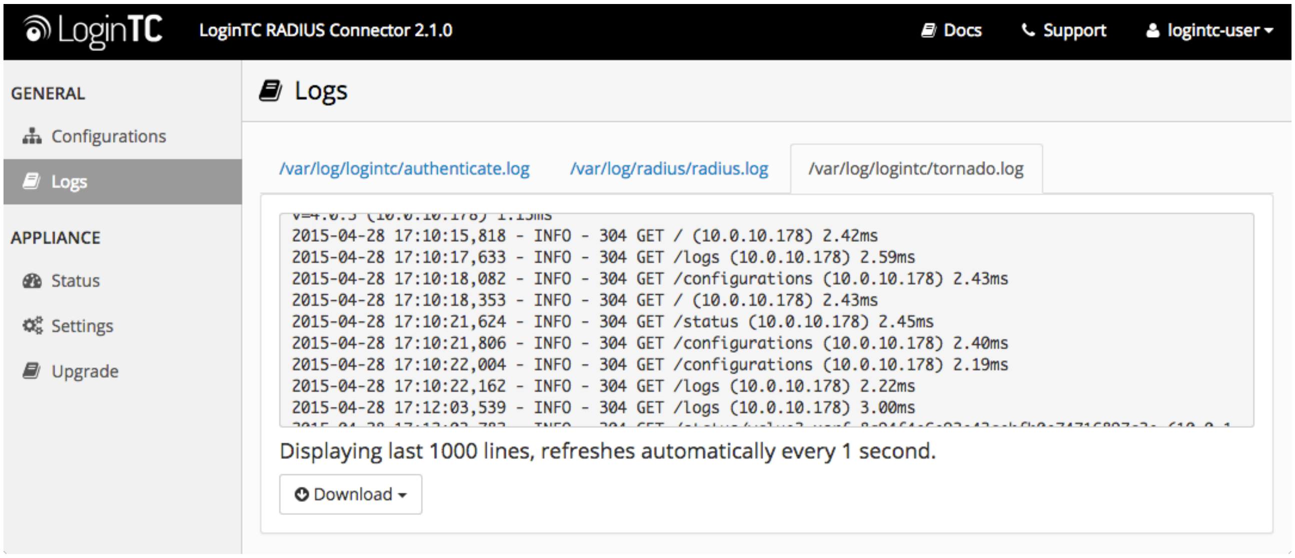


Status

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
/var/log/logintc/authenticate.log
/var/log/radius/radius.log
/var/log/logintc/tornado.log
Download

Logs

```
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.

Email Support

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