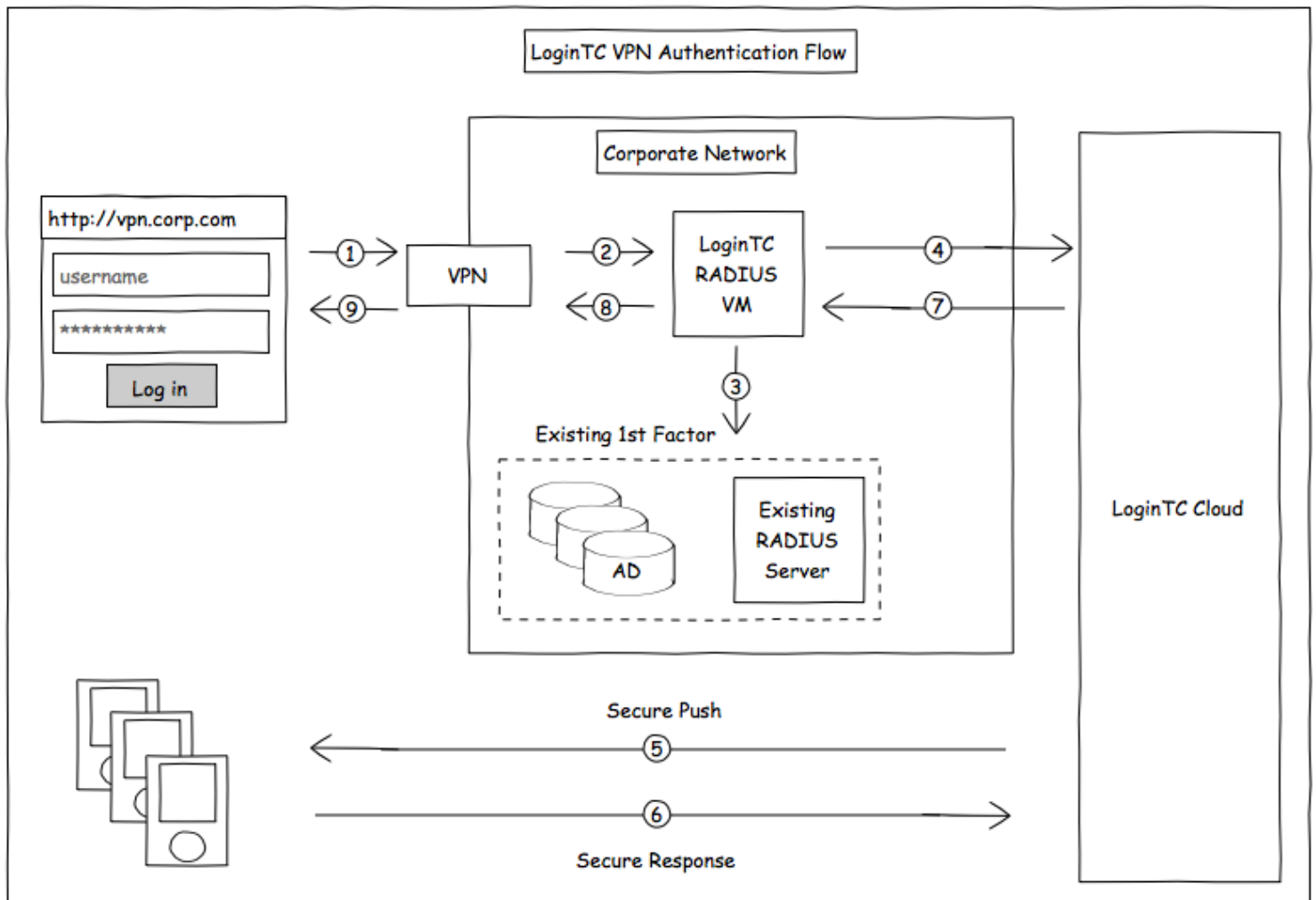


# Two factor authentication for Fortinet SSL VPN

[www.logintc.com/docs/connectors/fortinet.html](http://www.logintc.com/docs/connectors/fortinet.html)

## Introduction

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



## Prefer Reading a PDF?

Download a PDF file with configuration instructions for your chosen VPN protocol:

[Get the Fortinet SSL VPN with LoginTC guide for Two Factor Authentication](#)

## Compatibility

Fortinet appliance compatibility:

- FortiGate/FortiWifi 30-90 Entry-Level series
- FortiGate 100-900 Mid-Range series

- FortiGate 1000-5000 High-End series
- Fortinet/FortiGate appliance supporting RADIUS authentication

## Compatibility Guide

Fortinet appliances which have configurable RADIUS authentication are supported.

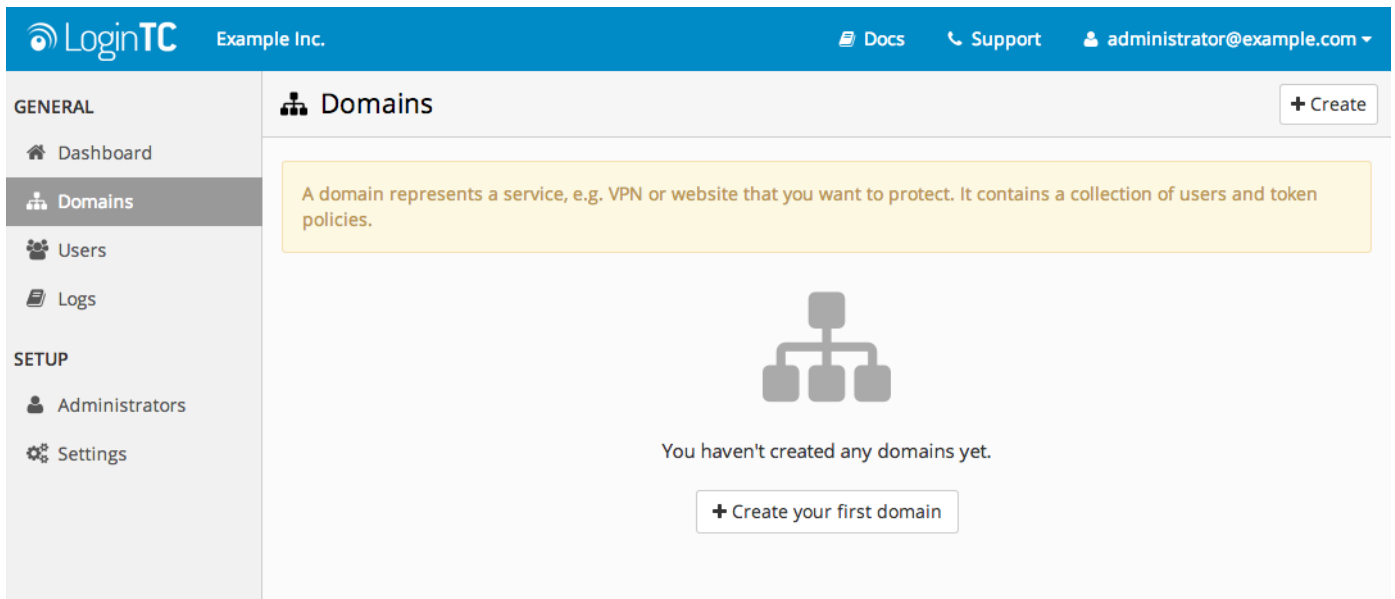
### Prerequisites

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**:



4. Enter domain information:

 Example Inc.
 
[Docs](#)
[Support](#)
administrator@example.com

---

**GENERAL**

- [Dashboard](#)
- [Domains](#)
- [Users](#)
- [Logs](#)

**SETUP**

- [Administrators](#)
- [Settings](#)

[Cancel](#)

### Domains / Create Domain

**Name** Name


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



---

**Icon**  Default  Custom

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




---

**Connector**  RADIUS  API  OpenAM  SiteMinder  Drupal  WordPress  Joomla

How you will connect your infrastructure to this domain

## RADIUS

Use the [RADIUS Connector](#) for your RADIUS appliance

---

**Key Policy**  PIN  Passcode

Specify how your users will unlock their token to authenticate

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

---

[Create](#)

## Name

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

## Connector

RADIUS

## Installation

The LoginTC RADIUS Connector runs [CentOS 6.5](#) with [SELinux](#). A firewall runs with the following open ports:

22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
80	TCP	Package updates (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.

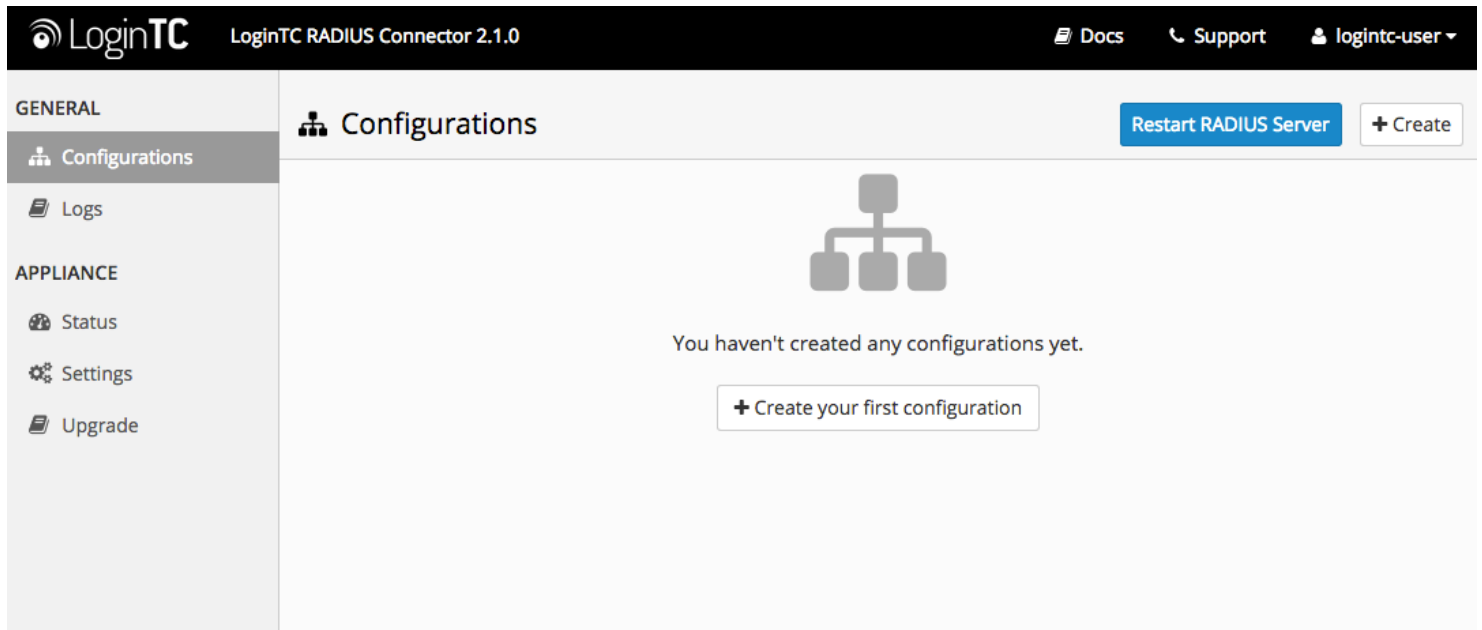
The **web interface** makes setting up a configuration simple and straightforward. Each section has a **Test** feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

## First Configuration

Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the

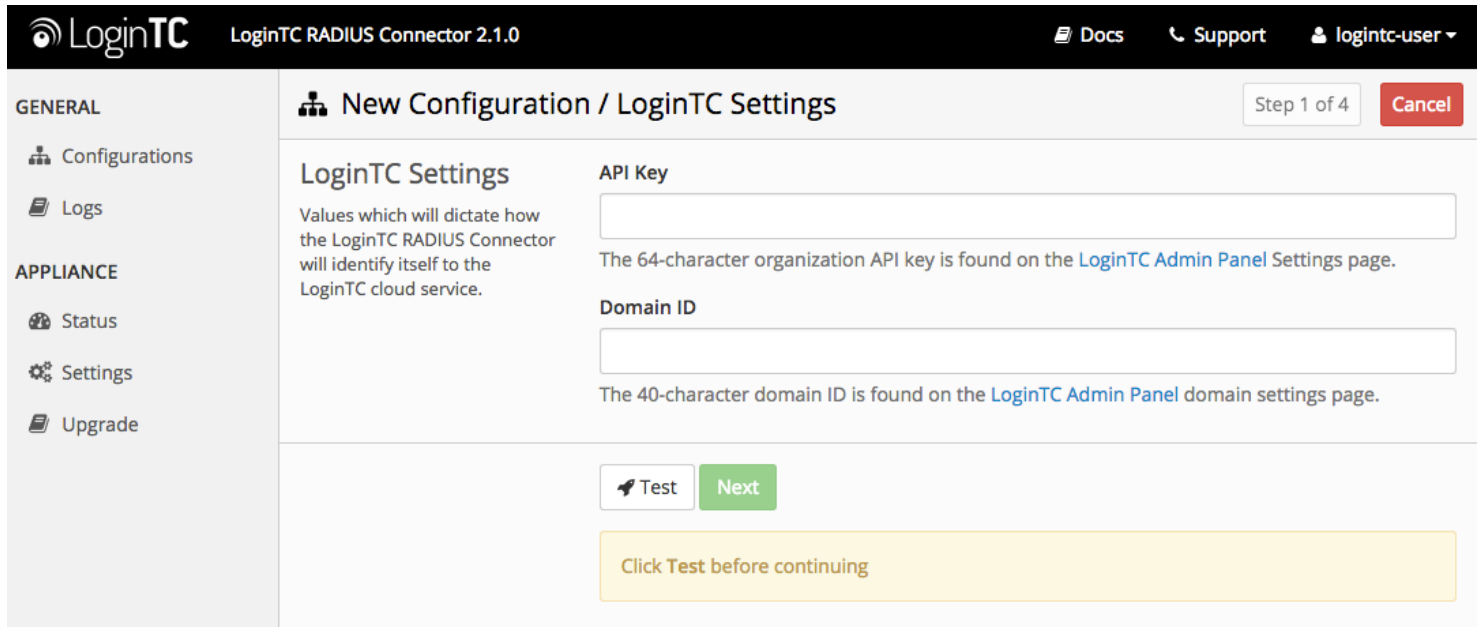
password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



## LoginTC Settings

Configure which LoginTC organization and domain to use:



Configuration values:

`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**:

The screenshot shows the 'New Configuration / LoginTC Settings' page in the LoginTC RADIUS Connector 2.1.0 interface. The page is titled 'Step 1 of 4' and includes a 'Cancel' button. The left sidebar shows 'GENERAL' with options for 'Configurations', 'Logs', 'APPLIANCE' with options for 'Status', 'Settings', and 'Upgrade'. The main content area is titled 'LoginTC Settings' and contains the following fields:

- API Key:** A text input field containing the value 'vZkDw7l6Z3tApwZjXERseKdR0s5RNNqjMxXlwwxpWwJ0a9oJXi9b5tdvPyFsqzWj'. Below the field is a note: 'The 64-character organization API key is found on the [LoginTC Admin Panel Settings](#) page.'
- Domain ID:** A text input field containing the value '9120580e94f134cb7c9f27cd1e43dbc82980e152'. Below the field is a note: 'The 40-character domain ID is found on the [LoginTC Admin Panel domain settings](#) page.'

At the bottom of the configuration area, there are two buttons: 'Test' and 'Next'. Below these buttons is a green message box that reads: 'Test successful, click Next to continue'.

## First Authentication Factor

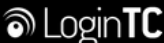
Configure the first authentication factor to be used in conjunction with LoginTC. You may use Active Directory / LDAP or an existing RADIUS server. You may also opt not to use a first factor, in which case LoginTC will be the only authentication factor.

The screenshot shows the 'New Configuration / First Factor' page in the LoginTC RADIUS Connector 2.1.0 interface. The page is titled 'Step 2 of 4' and includes a 'Cancel' button. The left sidebar is identical to the previous screenshot. The main content area is titled 'First Factor' and contains the following options and fields:

- First Factor:** A selection of radio buttons:  LDAP,  Active Directory,  RADIUS, and  None. Below the selection is a note: 'Connect to an existing LDAP server for username / password verification.'
- LDAP Server Details:** A section for configuring LDAP server information.
  - Host:** A text input field. Below the field is a note: 'Host name or IP address of the LDAP server. Examples: ldap.example.com or 192.168.1.42'
  - Port (optional):** A text input field containing the value '389'. Below the field is a note: 'Port if LDAP server uses non-standard port.'
- Bind Details:** A selection of radio buttons:  Bind with credentials and  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**:


LoginTC RADIUS Connector 2.1.0

[Docs](#)
[Support](#)
logintc-user

---

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**New Configuration / First Factor**
Step 2 of 4 Cancel

**First Factor**     LDAP     Active Directory     RADIUS     None

Select the first way users will authenticate prior to LoginTC.    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)**

Port if Active Directory server uses non-standard port.

---

**Bind Details**     Bind with credentials     Anonymous

Configuration values:

<code>host</code>	Host or IP address of the LDAP server	<code>ldap.example.com</code> or <code>192.168.1.42</code>
<code>port (optional)</code>	Port if LDAP server uses non-standard (i.e., <code>389/636</code> )	<code>4000</code>
<code>bind_dn</code>	DN of a user with read access to the directory	<code>cn=admin,dc=example,dc=com</code>
<code>bind_password</code>	The password for the above <code>bind_dn</code> account	<code>password</code>
<code>base_dn</code>	The top-level DN that you wish to query from	<code>dc=example,dc=com</code>
<code>attr_username</code>	The attribute containing the user's username	<code>sAMAccountName</code> or <code>uid</code>
<code>attr_name</code>	The attribute containing the user's real name	<code>displayName</code> or <code>cn</code>
<code>attr_email</code>	The attribute containing the user's email address	<code>mail</code> or <code>email</code>
<code>Group Attribute (optional)</code>	Specify an additional user group attribute to be returned the authenticating server.	<code>4000</code>
<code>RADIUS Group Attribute (optional)</code>	Name of RADIUS attribute to send back	<code>Filter-Id</code>
<code>LDAP Group (optional)</code>	The name of the LDAP group to be sent back to the authenticating server.	<code>SSLVPN-Users</code>
<code>encryption (optional)</code>	Encryption mechanism	<code>ssl</code> or <code>startTLS</code>
<code>cacert (optional)</code>	CA certificate file (PEM format)	<code>/opt/logintc/cacert.pem</code>

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**:

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

**New Configuration / First Factor** Step 2 of 4 **Cancel**

**First Factor**  LDAP  Active Directory  RADIUS  None

Select the first way users will authenticate prior to LoginTC. 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)**  
Port if the RADIUS server uses non-standard port.

**Secret**

Configuration values:

<code>host</code>	Host or IP address of the RADIUS server	<code>radius.example.com</code> or <code>192.168.1.43</code>
<code>port</code> (optional)	Port if the RADIUS server uses non-standard (i.e., 1812)	<code>6812</code>
<code>secret</code>	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	<code>testing123</code>

## 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.

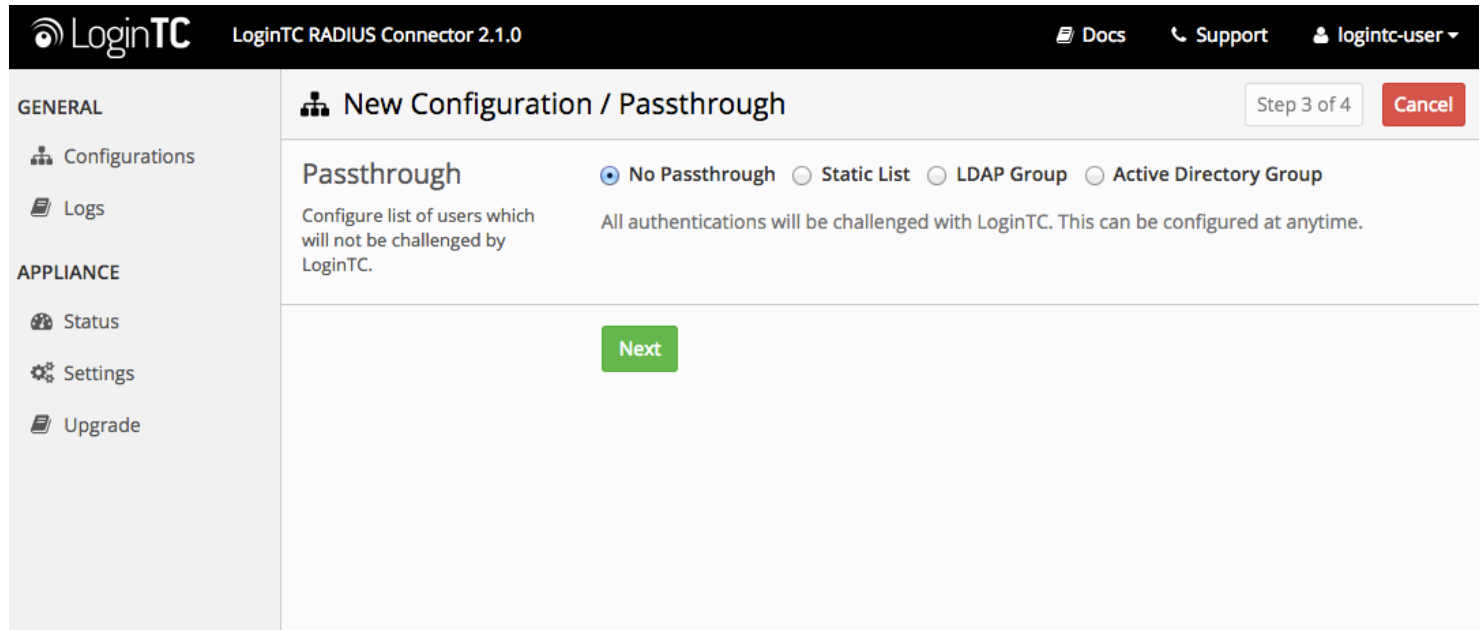
For larger deployments you can elect to use the [Active Directory or LDAP Group](#) option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC



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)

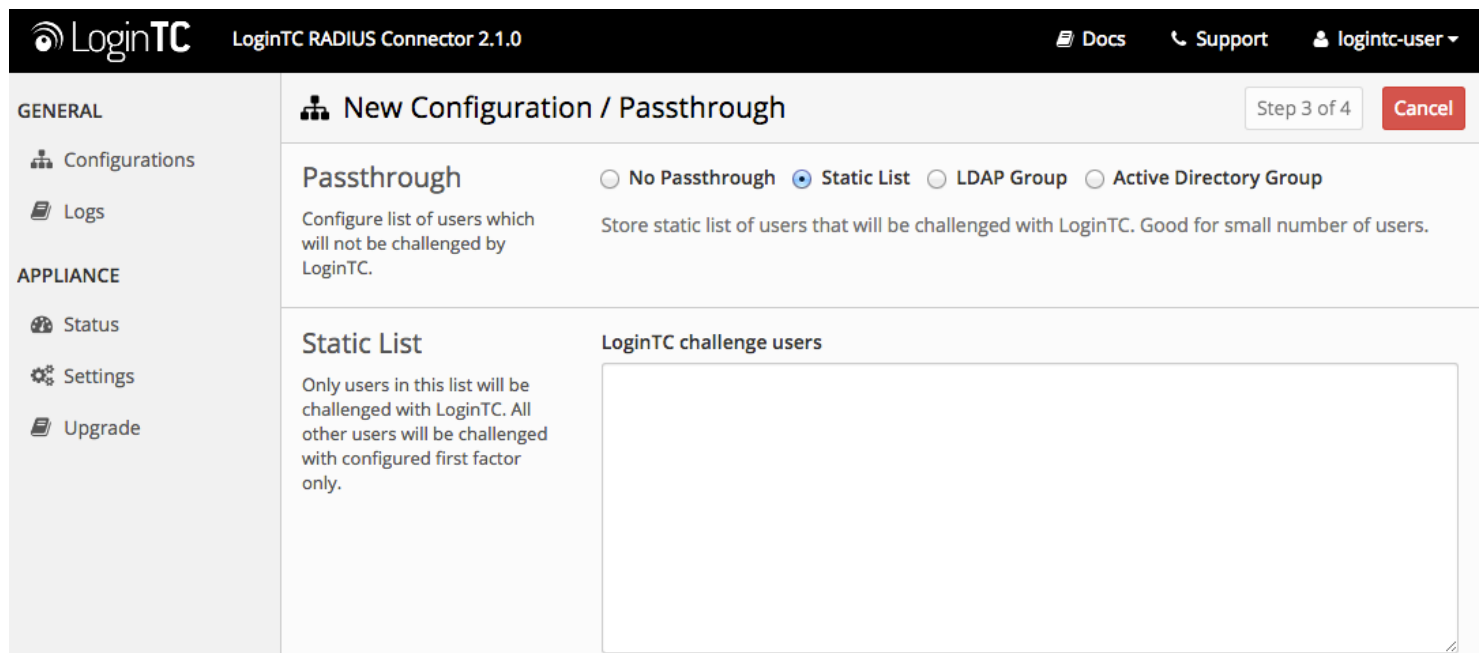
Select this option if you wish every user to be challenged with LoginTC.



The screenshot shows the LoginTC RADIUS Connector 2.1.0 interface. The top navigation bar includes the LoginTC logo, version information, and links for Docs, Support, and a user profile. A left sidebar contains menu items for GENERAL (Configurations, Logs) and APPLIANCE (Status, Settings, Upgrade). The main content area is titled 'New Configuration / Passthrough' and indicates 'Step 3 of 4'. Under the 'Passthrough' heading, four radio button options are visible: 'No Passthrough' (selected), 'Static List', 'LDAP Group', and 'Active Directory Group'. A descriptive text states: 'Configure list of users which will not be challenged by LoginTC. All authentications will be challenged with LoginTC. This can be configured at anytime.' A green 'Next' button is positioned below the text.

## 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.



The screenshot shows the LoginTC RADIUS Connector 2.1.0 interface with the 'Static List' option selected. The 'Passthrough' section now shows 'Static List' as the selected radio button. The descriptive text reads: 'Store static list of users that will be challenged with LoginTC. Good for small number of users.' Below this, a new section titled 'Static List' is visible, with the text: 'Only users in this list will be challenged with LoginTC. All other users will be challenged with configured first factor only.' To the right of this text is a large, empty text area labeled 'LoginTC challenge users' for entering the list of usernames.

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.

The screenshot shows the 'New Configuration / Passthrough' configuration page in the LoginTC RADIUS Connector 2.1.0. The page is divided into three main sections: 'Passthrough', 'Auth Groups', and 'AD Server Details'. The 'Passthrough' section has four radio button options: 'No Passthrough', 'Static List', 'LDAP Group', and 'Active Directory Group', with 'Active Directory Group' selected. Below this, there is a text input field for 'LoginTC challenge Auth Groups' and a description: 'Connect to an existing Active Directory server for group membership verification. Good for large number of users.' The 'Auth Groups' section has a text input field and a description: '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.' The 'AD Server Details' section has a text input field for 'Host' and a description: 'The Active Directory host and port information.'

Configuration values:

<code>LoginTC challenge auth groups</code>	Comma separated list of groups for which users will be challenged with LoginTC	<code>SSLVPN-Users</code> or <code>two-factor-users</code>
<code>host</code>	Host or IP address of the LDAP server	<code>ldap.example.com</code> or <code>192.168.1.42</code>
<code>port (optional)</code>	Port if LDAP server uses non-standard (i.e., <code>389</code> / <code>636</code> )	<code>4000</code>
<code>bind_dn</code>	DN of a user with read access to the directory	<code>cn=admin,dc=example,dc=com</code>
<code>bind_password</code>	The password for the above <code>bind_dn</code> account	<code>password</code>
<code>base_dn</code>	The top-level DN that you wish to query from	<code>dc=example,dc=com</code>
<code>attr_username</code>	The attribute containing the user's username	<code>sAMAccountName</code> or <code>uid</code>
<code>attr_name</code>	The attribute containing the user's real name	<code>displayName</code> or <code>cn</code>
<code>attr_email</code>	The attribute containing the user's email address	<code>mail</code> or <code>email</code>

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

## 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):

Client configuration values:

<code>name</code>	A unique identifier of your RADIUS client	<code>CorporateVPN</code>
<code>ip</code>	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	<code>192.168.1.44</code>
<code>secret</code>	The secret shared between the LoginTC RADIUS Connector and its client	<code>bigsecret</code>

## 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**.

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

Configurations

Restart RADIUS Server

+ Create

Configuration office-vpn-1 created

office-vpn-1 (Office VPN)

RADIUS

Test Configuration

## 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:

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

Configurations

Restart RADIUS Server

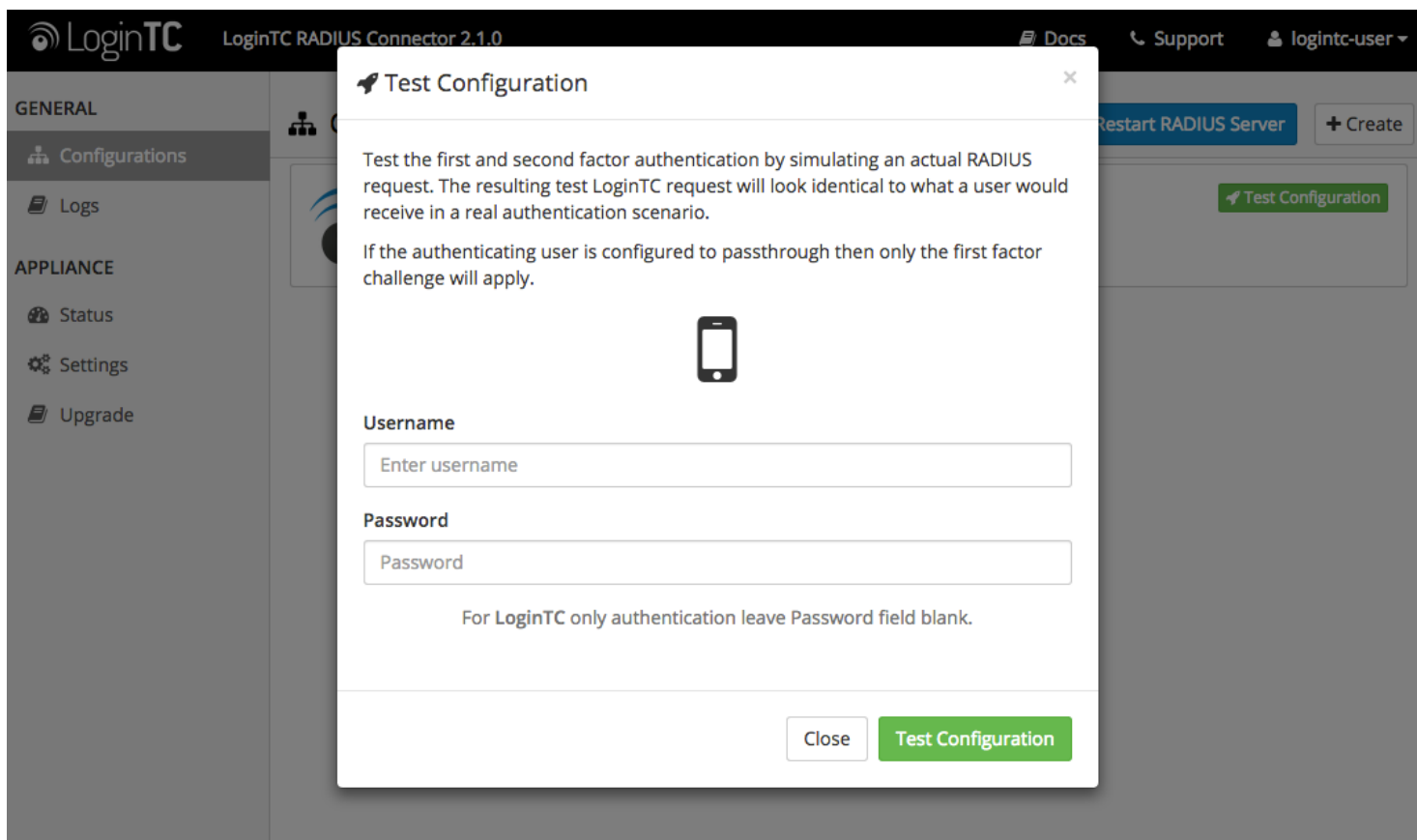
+ Create

office-vpn-1 (Office VPN)

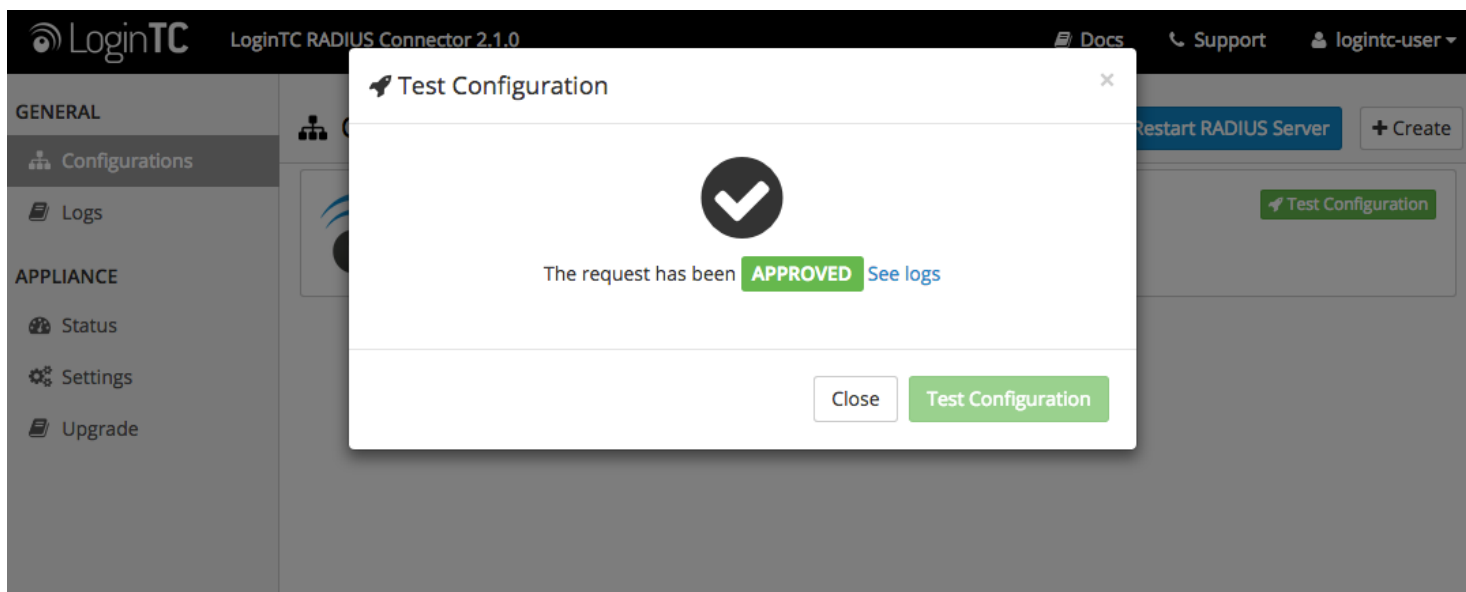
RADIUS

Test Configuration

Click **Test Configuration**:

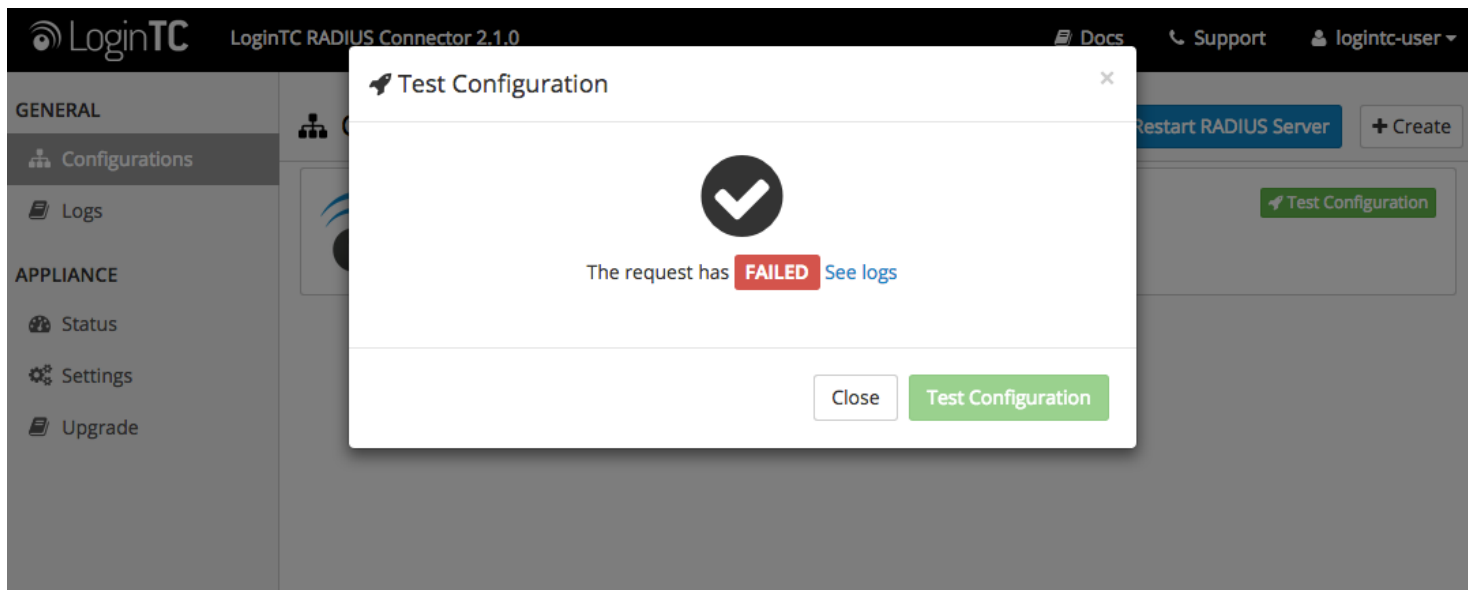


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

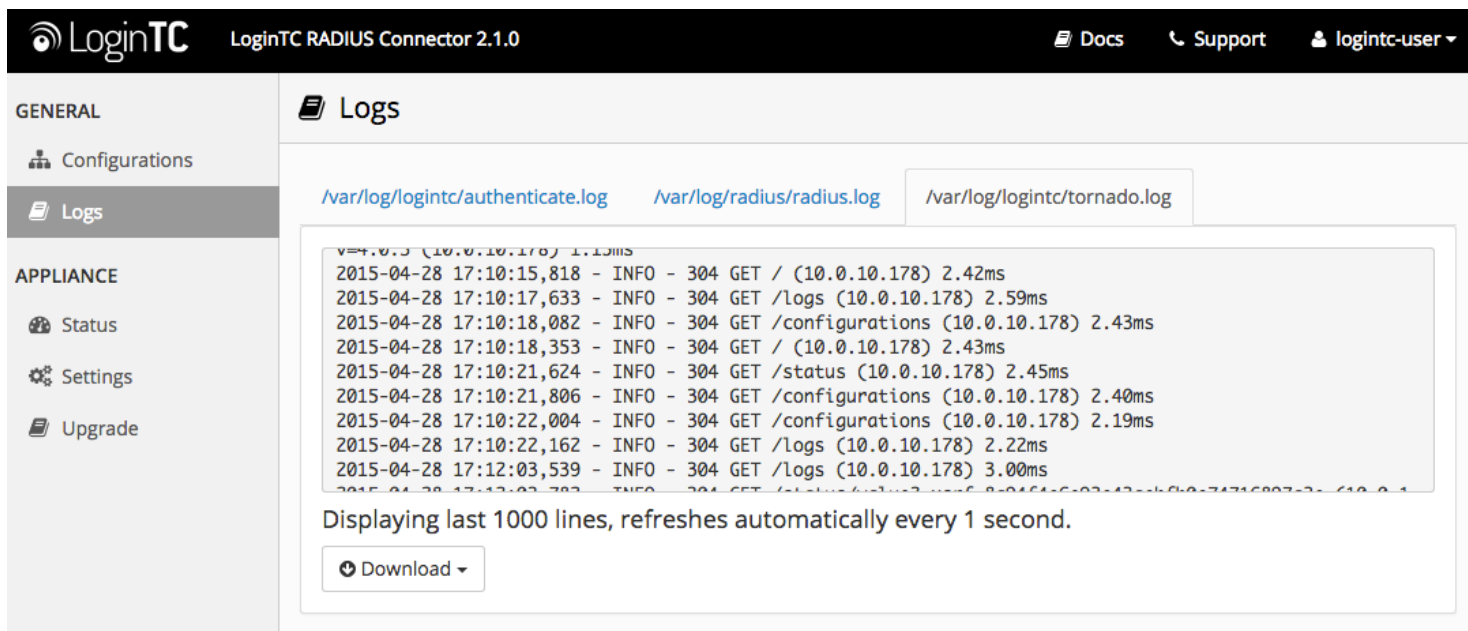


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



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



## Fortinet Configuration - Quick Guide

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

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

LoginTC LoginTC RADIUS Connector 2.1.0 Docs Support logintc-user

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings**
- Upgrade

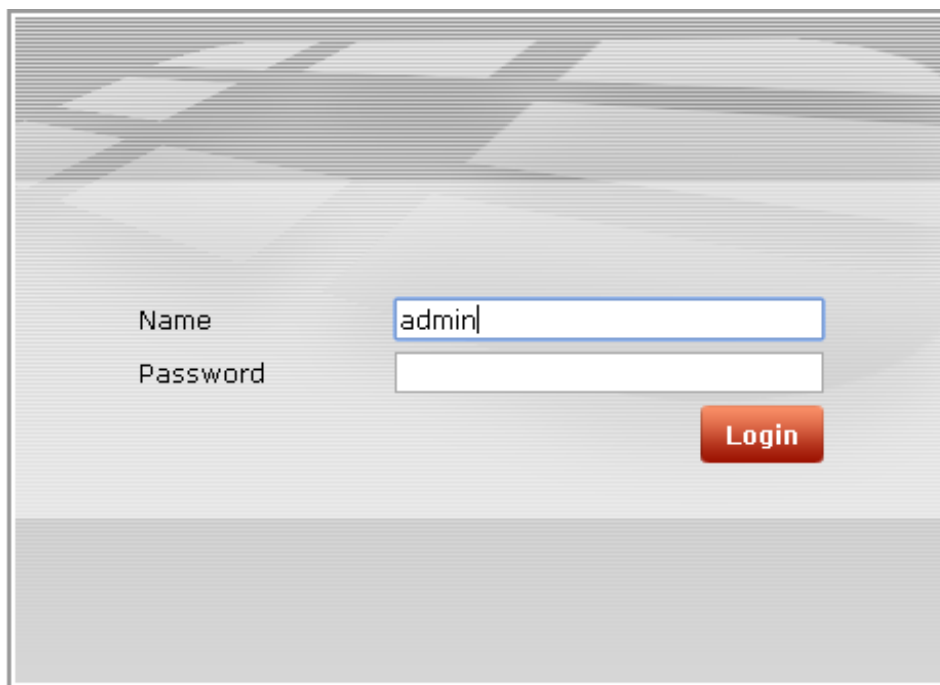
### Settings

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 Fortinet web manager (<https://<IP address for the Fortinet web manager>>)



2. Navigate to **System > Dashboard > Status** and scroll down to **CLI Console**:

The screenshot shows the FortiGate VM64 management interface. The left sidebar contains a 'System' menu with options: Dashboard, Status (selected), FortiView, Network, Config, Admin, Certificates, and Monitor. Below this are sections for Router, Policy & Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The main content area features a 'Widget' and 'Dashboard' header. It includes a 'FortiClient' widget with 'FortiClient Installers' and 'Enter License' buttons for Mac and Windows. A 'FortiToken Mobile' widget shows 'Assigned / Allowed' with a counter '0 of 2'. A 'CLI Console' window is open, displaying 'Connected' and the device ID 'FGVM00000034732 #'. Below the console, 'System Resources' are shown with 'CPU Usage: 3%' and 'Memory Usage: 44%'.

3. Run the following commands in the console:

```
# config system
global
# set remoteauthtimeout
60
#
end
```

The screenshot shows the CLI Console window with the following text:

```
Connected

FGVM00000034732 # config system global

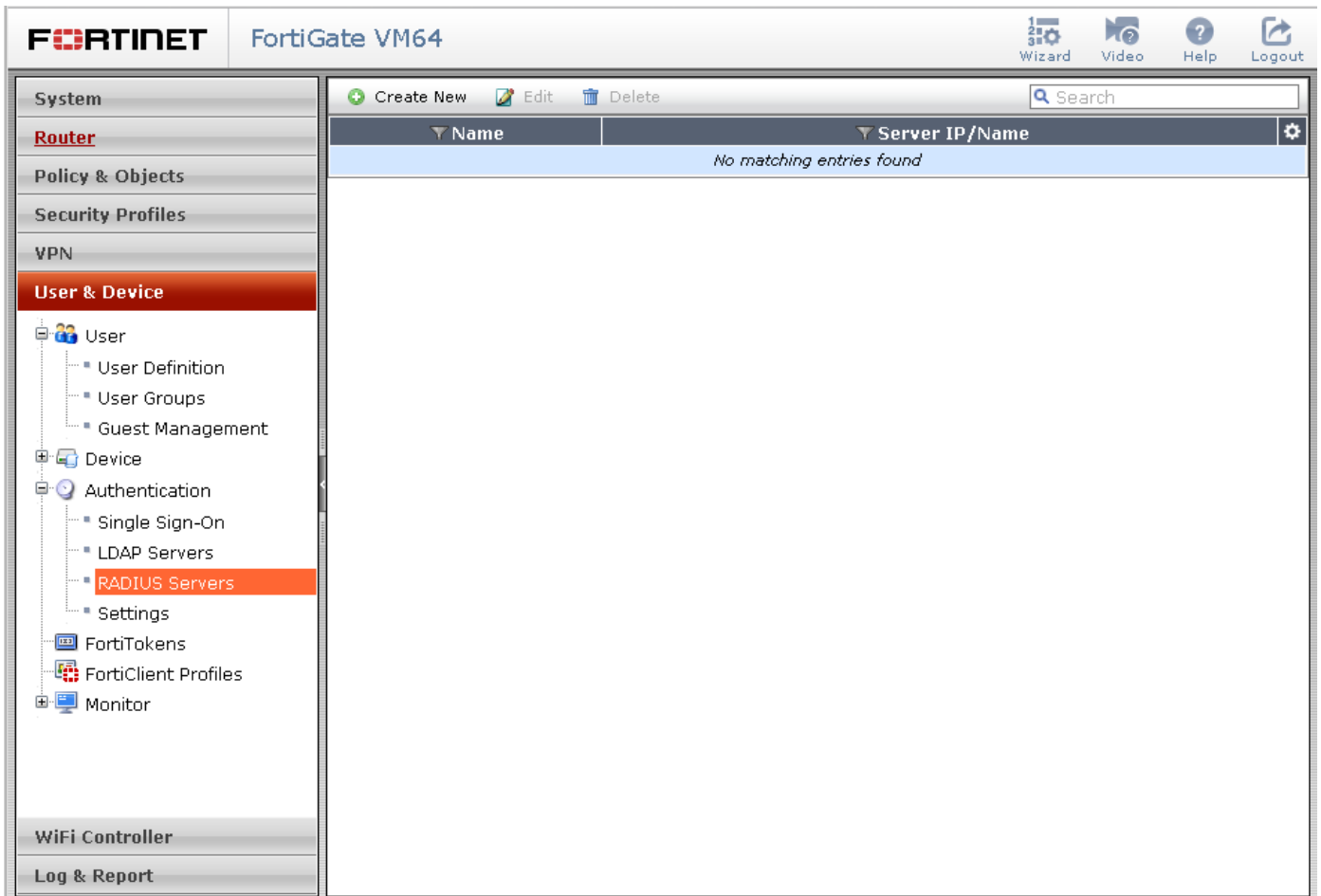
FGVM00000034732 (global) # set remoteauthtimeout 60

FGVM00000034732 (global) # end

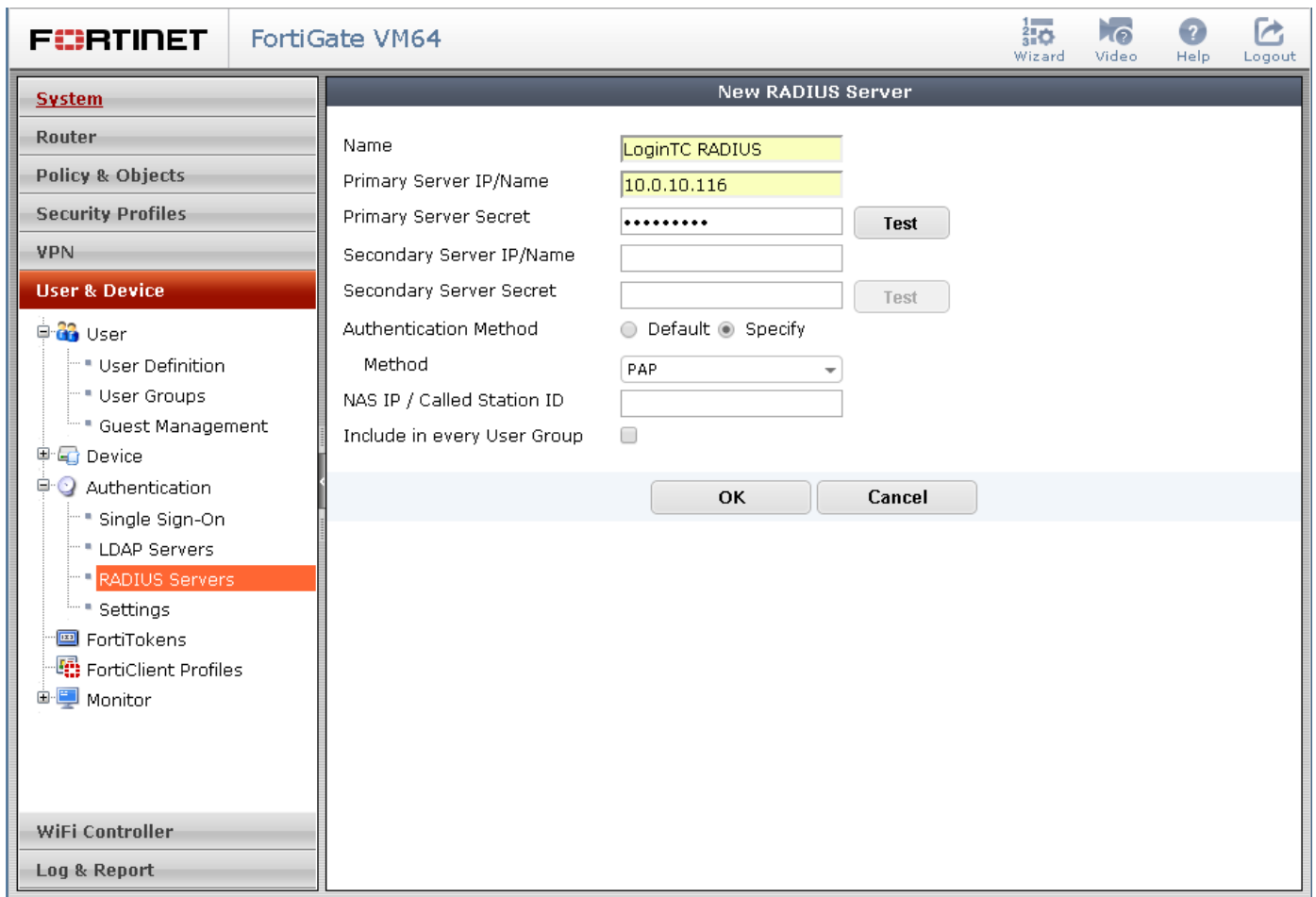
FGVM00000034732 #
```



4. Navigate to **User & Device > Authentication > RADIUS Servers** and click on **Create New** button:



5. Complete the form and click **OK** (click the **Test** button beside **Primary Server Secret** to test the setup):



Primary Server IP/Name	Address of LoginTC RADIUS Connector	10.0.10.116
Primary Server Secret	The secret shared between the LoginTC RADIUS Connector and its client.	bigsecret
Secondary Server IP/Name	Secondary RADIUS Server IP. Optional.	
Secondary Server Secret	The secondary server secret. Optional.	
Authentication Method	RADUIS authentication method. Must be PAP.	PAP
NAS IP / Called Station ID	Network Access Server IP. Optional.	
Include in every User Group	Automatically included in all user groups. Optional.	

To test, navigate to your Fortinet VPN portal and attempt access.

## User Management

There are several options for managing your users within LoginTC:

## Troubleshooting

### LoginTC RADIUS Connector Has 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
```

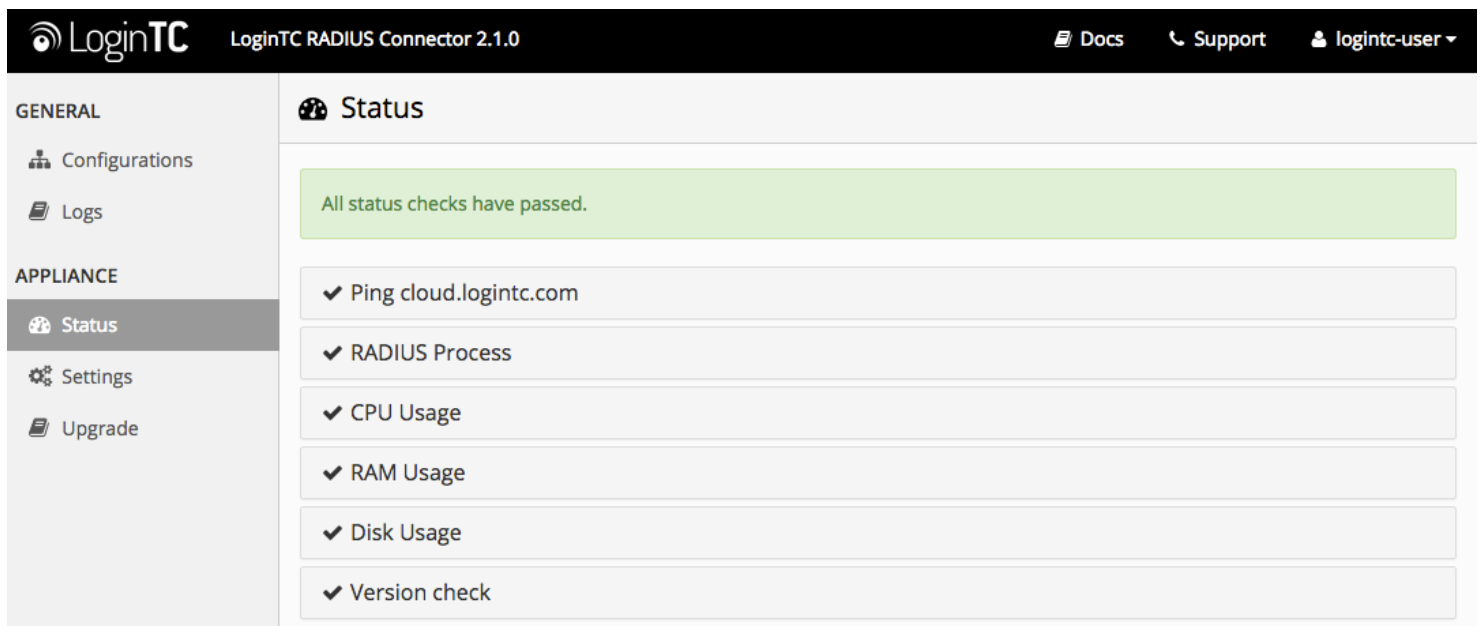
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

```
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"`

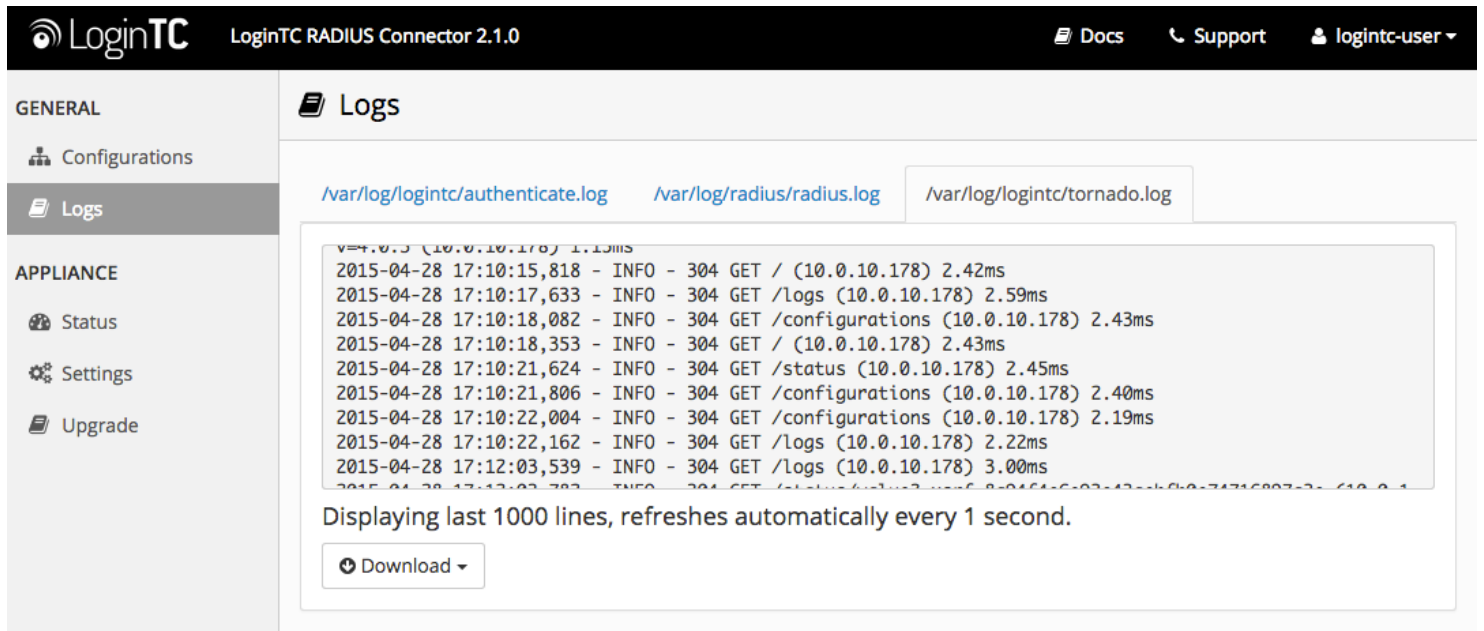
## Not Authenticating

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



The screenshot shows the LoginTC RADIUS Connector 2.1.0 web interface. The top navigation bar includes the LoginTC logo, the product name, and links for Docs, Support, and the user profile (logintc-user). The left sidebar contains a menu with 'GENERAL' (Configurations, Logs) and 'APPLIANCE' (Status, Settings, Upgrade). The main content area is titled 'Status' and displays a green message box stating 'All status checks have passed.' Below this, a list of checks is shown, each with a checkmark icon: 'Ping cloud.logintc.com', 'RADIUS Process', 'CPU Usage', 'RAM Usage', 'Disk Usage', and 'Version check'.

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



GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

Logs

[/var/log/logintc/authenticate.log](#) [/var/log/radius/radius.log](#) [/var/log/logintc/tornado.log](#)

```
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.

Download

## Email Support

For any additional help please email [support@cyphercor.com](mailto:support@cyphercor.com). Expect a speedy reply.

## Upgrading

If you have LoginTC RADIUS Connector 1.1.0 or higher, follow these instructions to upgrade your LoginTC RADIUS virtual appliance to the latest version (2.1.6.2):

1. SSH into the virtual appliance or open the console (use same username / password as web GUI)
2. `cd /tmp`  
`curl -O https://www.logintc.com/downloads/logintc-radius-connector-2.1.6.2-upgrade.sh`
3. `upgrade.sh`  
`sudo sh logintc-radius-connector-2.1.6.2-upgrade.sh`
4. `upgrade.sh`

The upgrade script will restart your appliance after upgrading.

## Upgrade Script Download Verification

Execute: `shasum /tmp/logintc-radius-connector-2.1.6.2-upgrade.sh`

Output SHA-1 should match: `868c4d6cb9699c769d17944566e41f86e8e0de36`