

Two factor authentication for RADIUS appliances

 www.logintc.com/docs/connectors/radius.html

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine appliance packaged to run within your corporate network. The LoginTC RADIUS Connector allows your **RADIUS**-speaking corporate resources (e.g. VPNs) to use **LoginTC** for the most secure two-factor authentication. Supported devices include :

- Cisco ACS / ISE / ISR / Catalyst / IPsec VPN/ SSH Network Device Access
- Citrix NetScaler Gateway (XenDesktop/XenApp)
- Palo Alto GlobalProtect / IPSEC VPN
- Dell SonicWALL NSA, TZ and Aventail (including Mobile Connect)
- VMware, Sohpos, F5, Pulse Secure, Array Networks, NetMotion

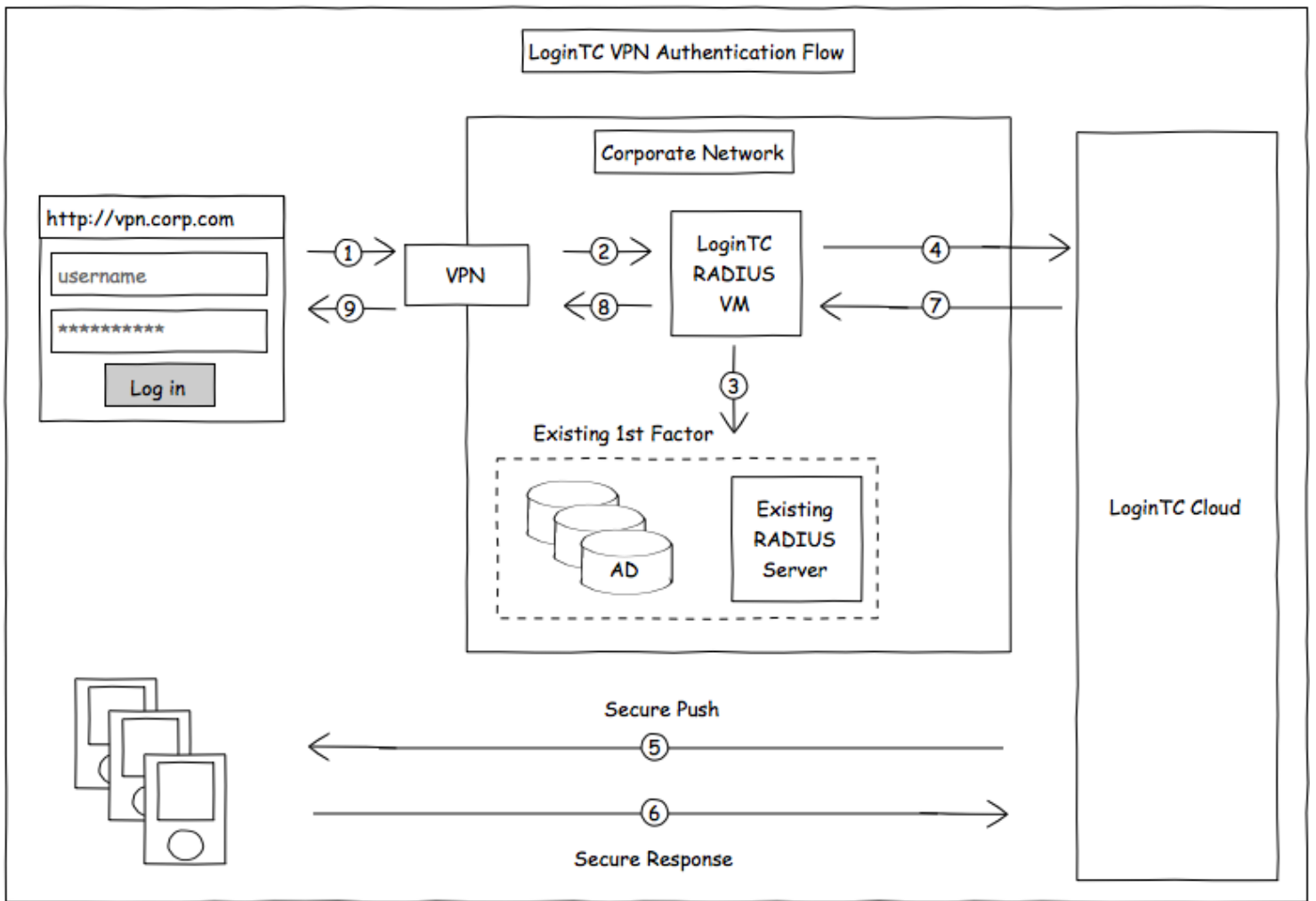
Any other appliances which have configurable RADIUS authentication are supported.

Since the LoginTC RADIUS Connector can speak RADIUS and LDAP it fits seamlessly into your existing setup without significant disruption. The appliance is configured to provide authentication to your existing **RADIUS**-speaking device and brokers first and second factor user authentication. The optional first factor is against an already existing LDAP, Active Directory or RADIUS device. The second factor is a secure authentication request to the user's mobile or desktop device.

The Appliance is very easy to configure with a rich web-based interface much like [LoginTC Admin](#).

Authentication Flow

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



Prerequisites


Before proceeding, please ensure you have the following:

RADIUS Domain Creation

Create a RADIUS domain in [LoginTC Admin](#). The domain represents a service (e.g. VPN) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

If you have already created a LoginTC 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 **Create Domain**:

 Example Inc.

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

GENERAL
+ Create

[Dashboard](#)

Domains

[Users](#)


[Logs](#)

SETUP

[Administrators](#)

[Settings](#)


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.

+ Create your first domain

4. Enter domain information:

 Example Inc.

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

GENERAL
Domains / Create Domain Cancel

[Dashboard](#)

Domains

[Users](#)

[Logs](#)

SETUP

[Administrators](#)


[Settings](#)

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

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)
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

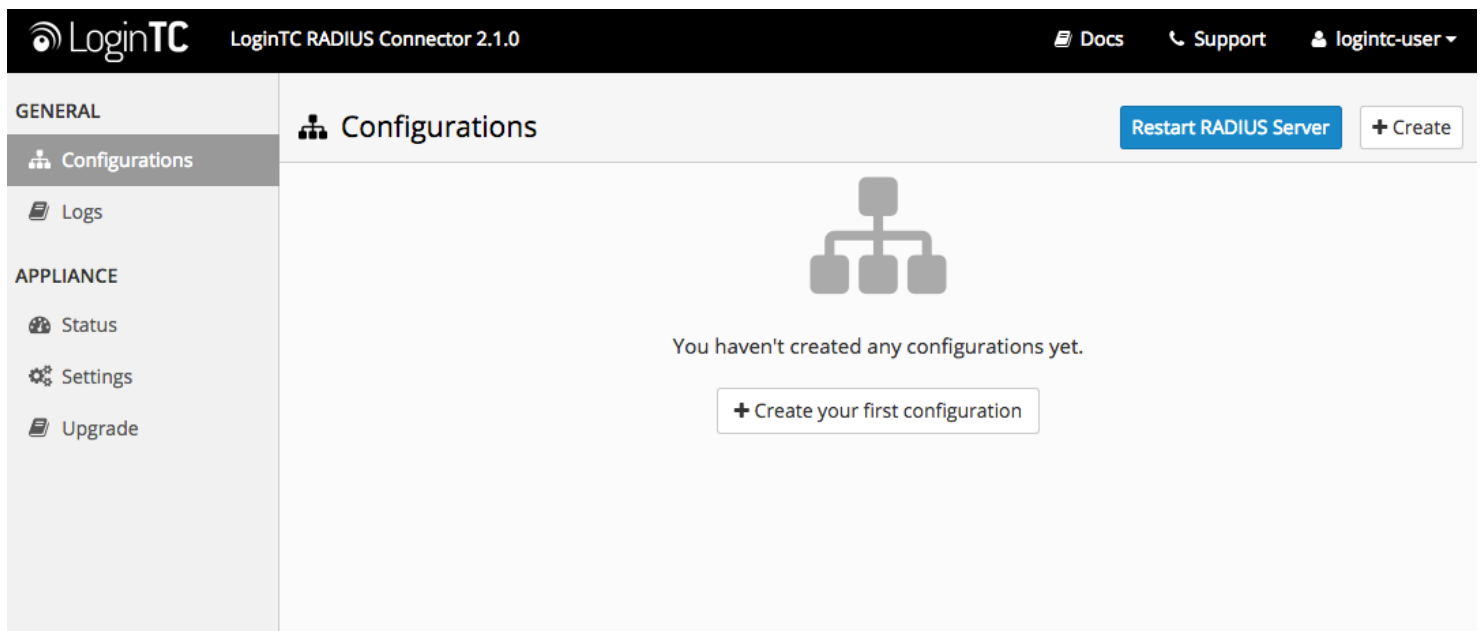
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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**:



LoginTC Settings

Configure which LoginTC organization and domain to use:

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

New Configuration / LoginTC Settings Step 1 of 4 **Cancel**

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.

Test **Next**

Click Test before continuing

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**:

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

New Configuration / LoginTC Settings Step 1 of 4 **Cancel**

LoginTC Settings

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

API Key

vZkDw7l6Z3tApwZJXERseKdR0s5RNNqjMxXlwxpWwJOa9oXl9b5tdvPyFsqzwJ

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 **Next**

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.





LoginTC RADIUS Connector 2.1.0

 Docs
  Support
  logintc-user

GENERAL

-  Configurations
-  Logs

APPLIANCE

-  Status
-  Settings
-  Upgrade

Step 2 of 4 Cancel

New Configuration / First Factor

First Factor
 LDAP
 Active Directory
 RADIUS
 None

Select the first way users will authenticate prior to LoginTC. Connect to an existing LDAP server for username / password verification.

LDAP Server Details
Host

The LDAP host and port information. Host name or IP address of the LDAP server. Examples: ldap.example.com or 192.168.1.42


Port (optional)




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**:





LoginTC RADIUS Connector 2.1.0

 Docs
  Support
  logintc-user

GENERAL

-  Configurations
-  Logs

APPLIANCE

-  Status
-  Settings
-  Upgrade

Step 2 of 4 Cancel

New Configuration / First Factor

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
Host

The Active Directory host and port information. 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</code> (optional)	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>
Group Attribute (optional)	Specify an additional user group attribute to be returned the authenticating server.	<code>4000</code>
RADIUS Group Attribute (optional)	Name of RADIUS attribute to send back	<code>Filter-Id</code>
LDAP Group (optional)	The name of the LDAP group to be sent back to the authenticating server.	<code>SSLVPN-Users</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>

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**:

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., <code>1812</code>)	<code>6812</code>

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.

The screenshot shows the configuration interface for the LoginTC RADIUS Connector. The top navigation bar includes the LoginTC logo, the version '2.1.0', and links for 'Docs', 'Support', and a user profile 'logintc-user'. The main content area is titled 'New Configuration / Passthrough' and is labeled as 'Step 3 of 4'. Under the 'Passthrough' heading, there are four radio button options: 'No Passthrough' (which is selected), 'Static List', 'LDAP Group', and 'Active Directory Group'. Below these options, a text box explains that this configuration is for users not challenged by LoginTC, and a note states that all authentications will be challenged with LoginTC. A green 'Next' button is positioned at the bottom of the configuration section.

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.

 LoginTC RADIUS Connector 2.1.0

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

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

Step 3 of 4 Cancel

New Configuration / Passthrough

Passthrough
 No Passthrough
 Static List
 LDAP Group
 Active Directory Group

Configure list of users which will not be challenged by LoginTC.
 Store static list of users that will be challenged with LoginTC. Good for small number of users.

Static List
LoginTC challenge users


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

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.

 LoginTC RADIUS Connector 2.1.0

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

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

Step 3 of 4 Cancel

New Configuration / Passthrough

Passthrough
 No Passthrough
 Static List
 LDAP Group
 Active Directory Group

Configure list of users which will not be challenged by LoginTC.
 Connect to an existing Active Directory server for group membership verification. Good for large number of users.

Auth Groups
LoginTC challenge 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.

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

AD Server Details
Host

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</code> (optional)	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):

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

New Configuration / Client and Encryption

Step 4 of 4

Cancel

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:

<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

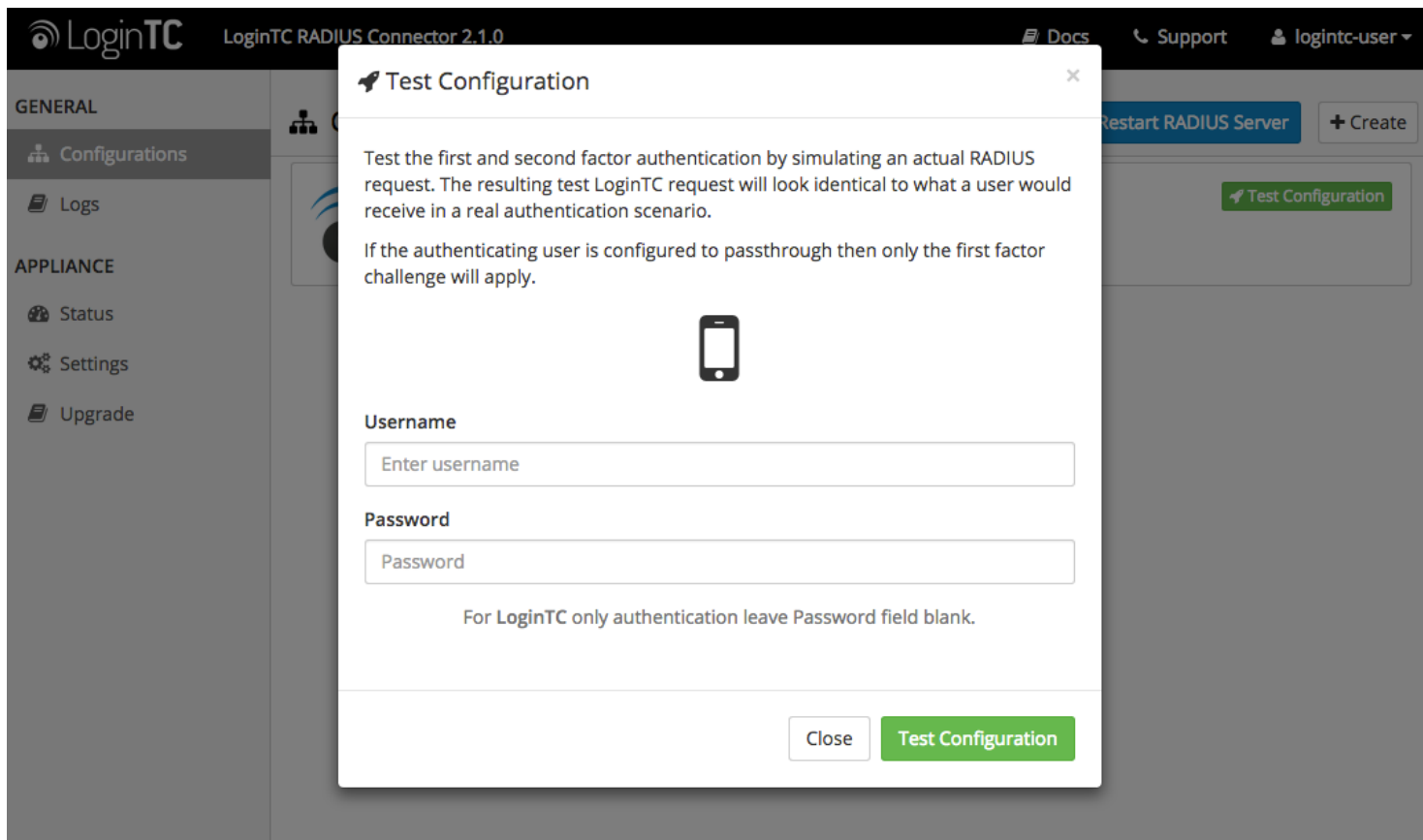
+ Create

office-vpn-1 (Office VPN)

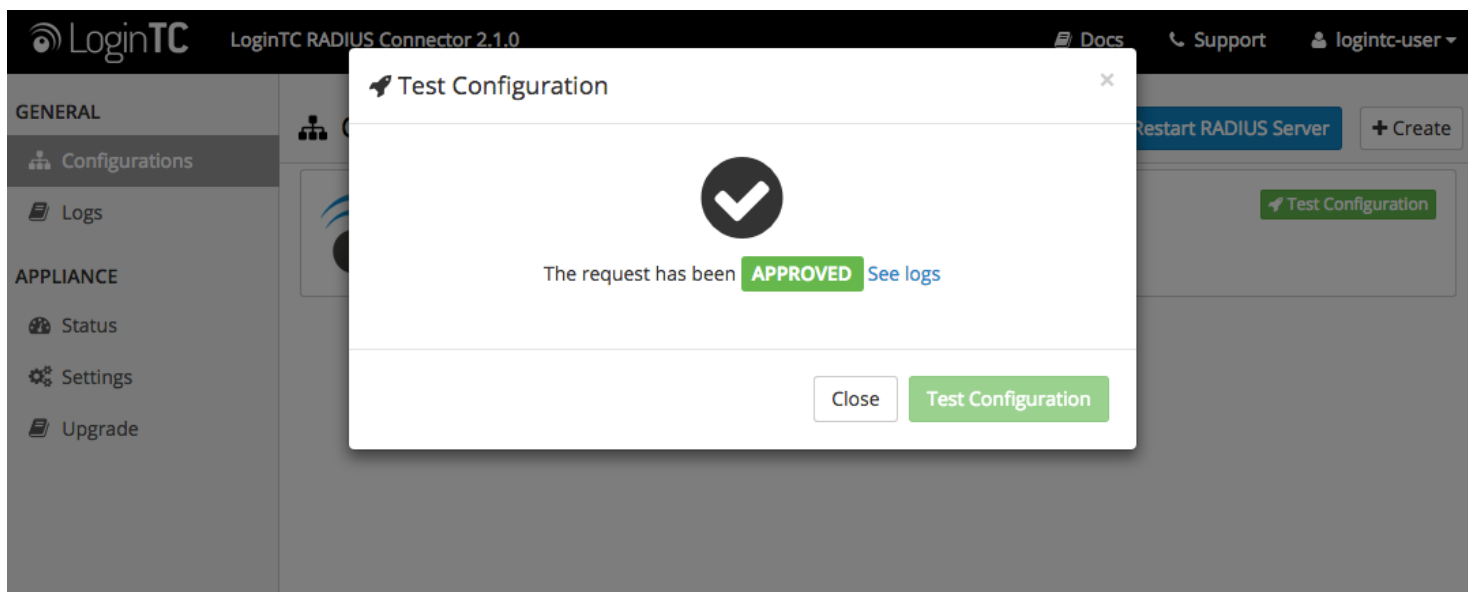
RADIUS

Test Configuration

Click **Test Configuration**:

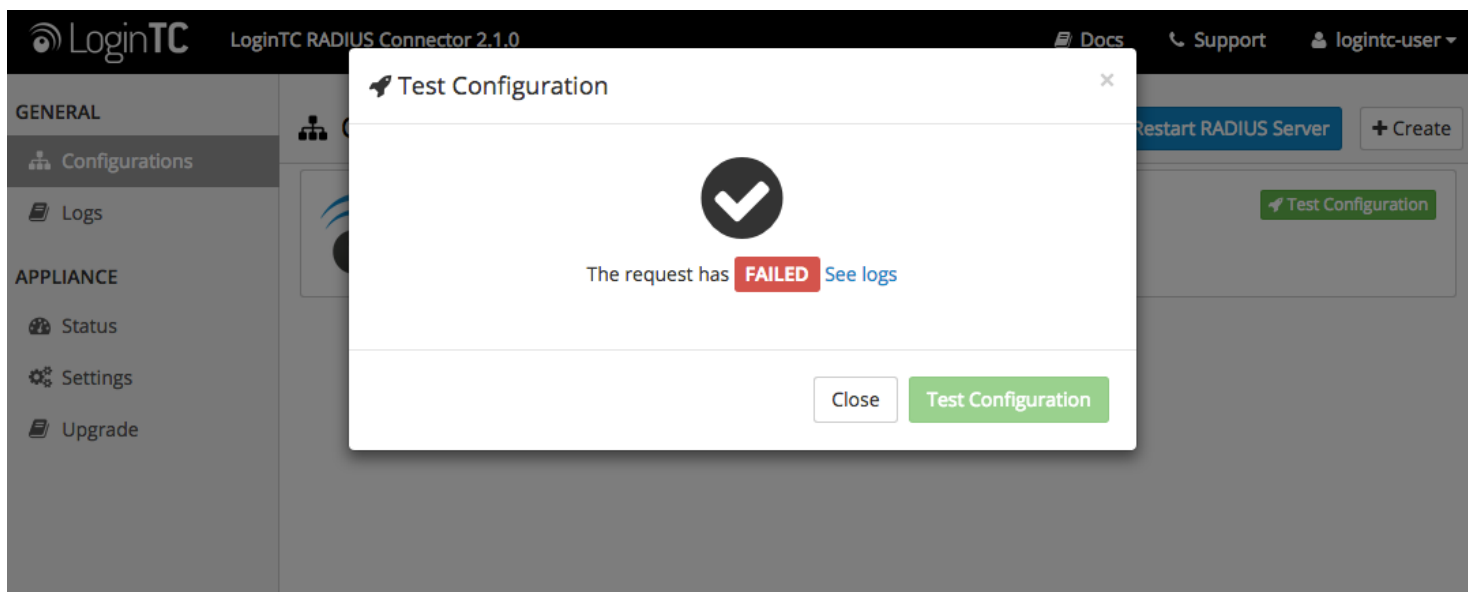


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

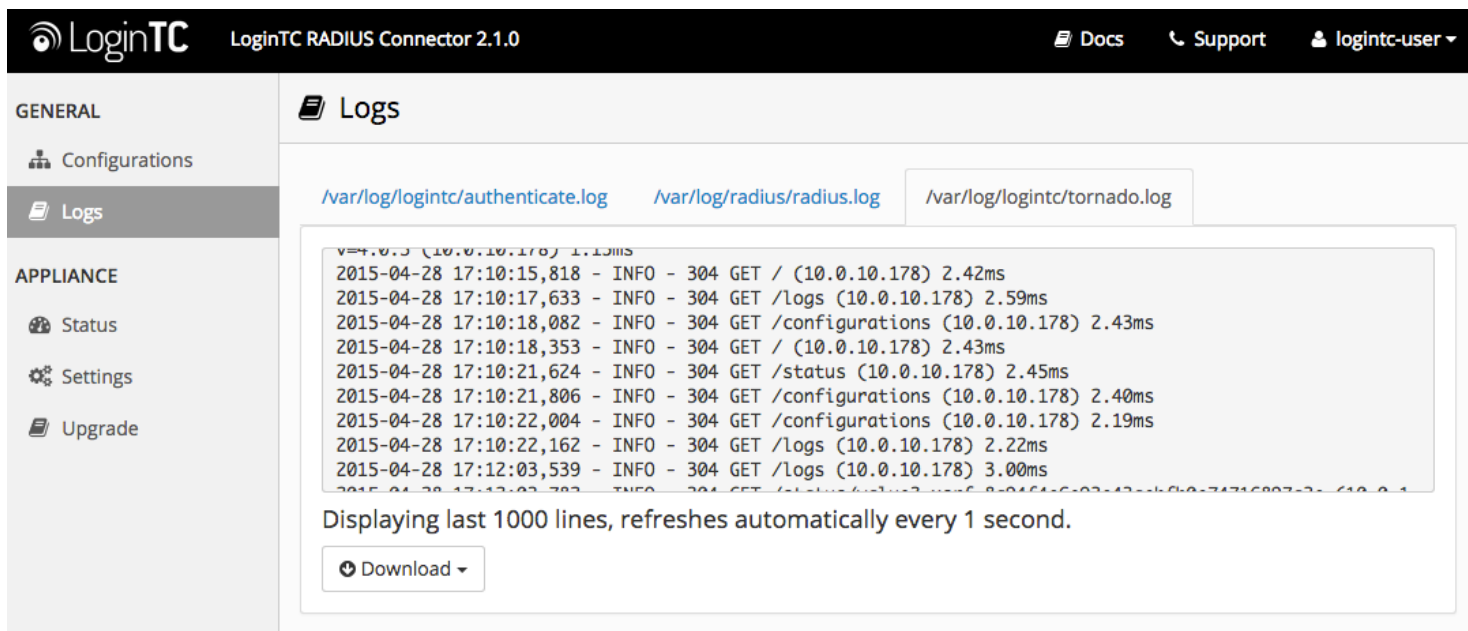


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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:



RADIUS Client Configuration

Once you are satisfied with your setup, configure your RADIUS device to use the LoginTC RADIUS Connector as its RADIUS authentication source. Set the RADIUS timeout to 60 seconds to allow enough time for LoginTC authentication responses.

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

User Management

Create users in LoginTC corresponding to your AD/LDAP users and provision them tokens. There are several options for managing your users within LoginTC:

For more details about user management and provisioning, visit the [User Management](#) guide.

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
```

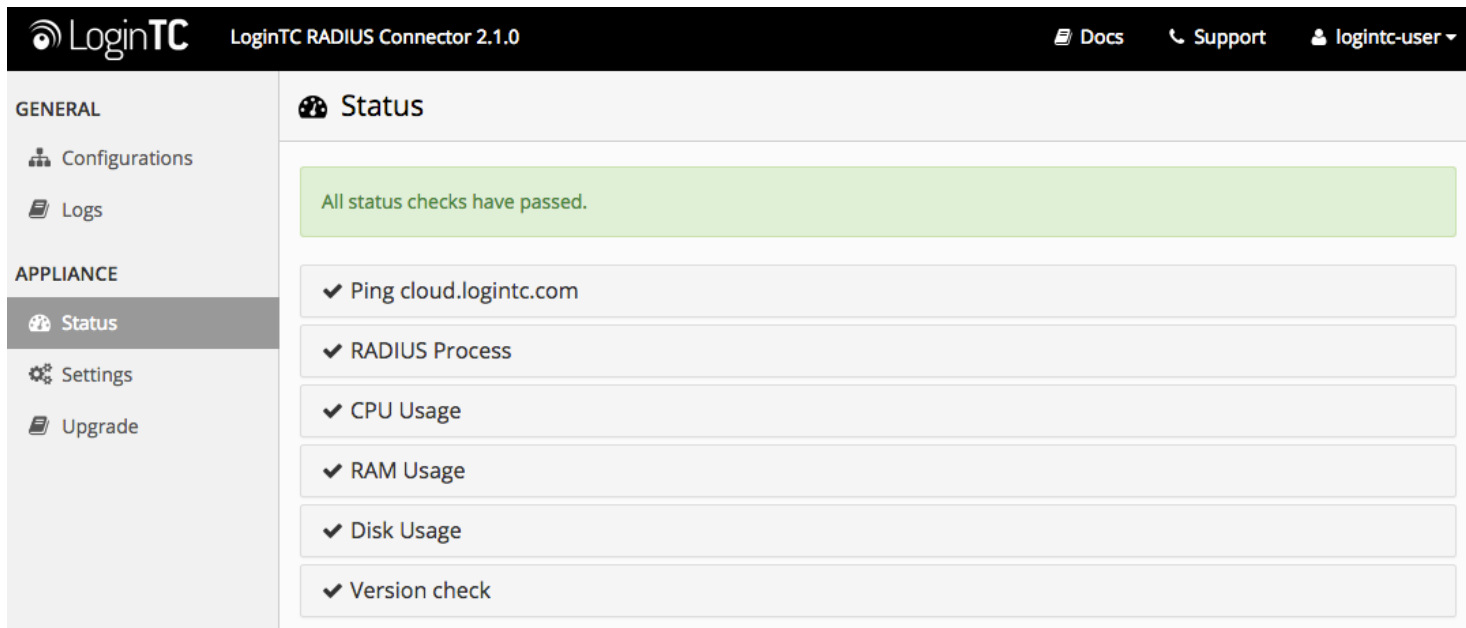
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

```
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"`

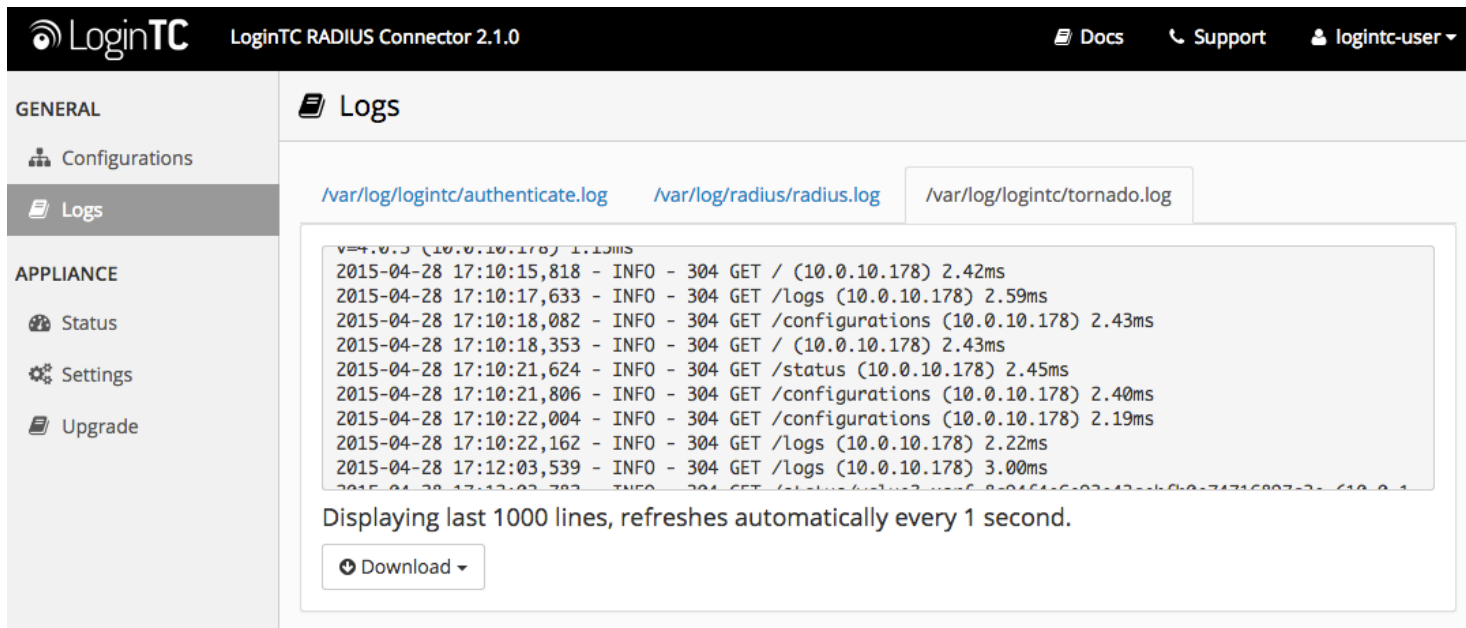
Not Authenticating

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



The screenshot shows the LoginTC web interface for the 'LoginTC RADIUS Connector 2.1.0'. The left sidebar has a 'GENERAL' section with 'Configurations' and 'Logs', and an 'APPLIANCE' section with 'Status', 'Settings', and 'Upgrade'. The 'Status' page is active, showing a green notification box: 'All status checks have passed.' Below this, there are seven status checks, each with a green checkmark: '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**:



The screenshot shows the LoginTC web interface for the 'LoginTC RADIUS Connector 2.1.0'. The left sidebar has a 'GENERAL' section with 'Configurations' and 'Logs', and an 'APPLIANCE' section with 'Status', 'Settings', and 'Upgrade'. The 'Logs' page is active, showing a list of log entries from the file '/var/log/logintc/authenticate.log'. The log entries show HTTP GET requests and their response times. Below the log entries, there is a message: 'Displaying last 1000 lines, refreshes automatically every 1 second.' and a 'Download' button.

Email Support

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