Two factor authentication for Remote Desktop Gateway (RD Gateway) with RADIUS

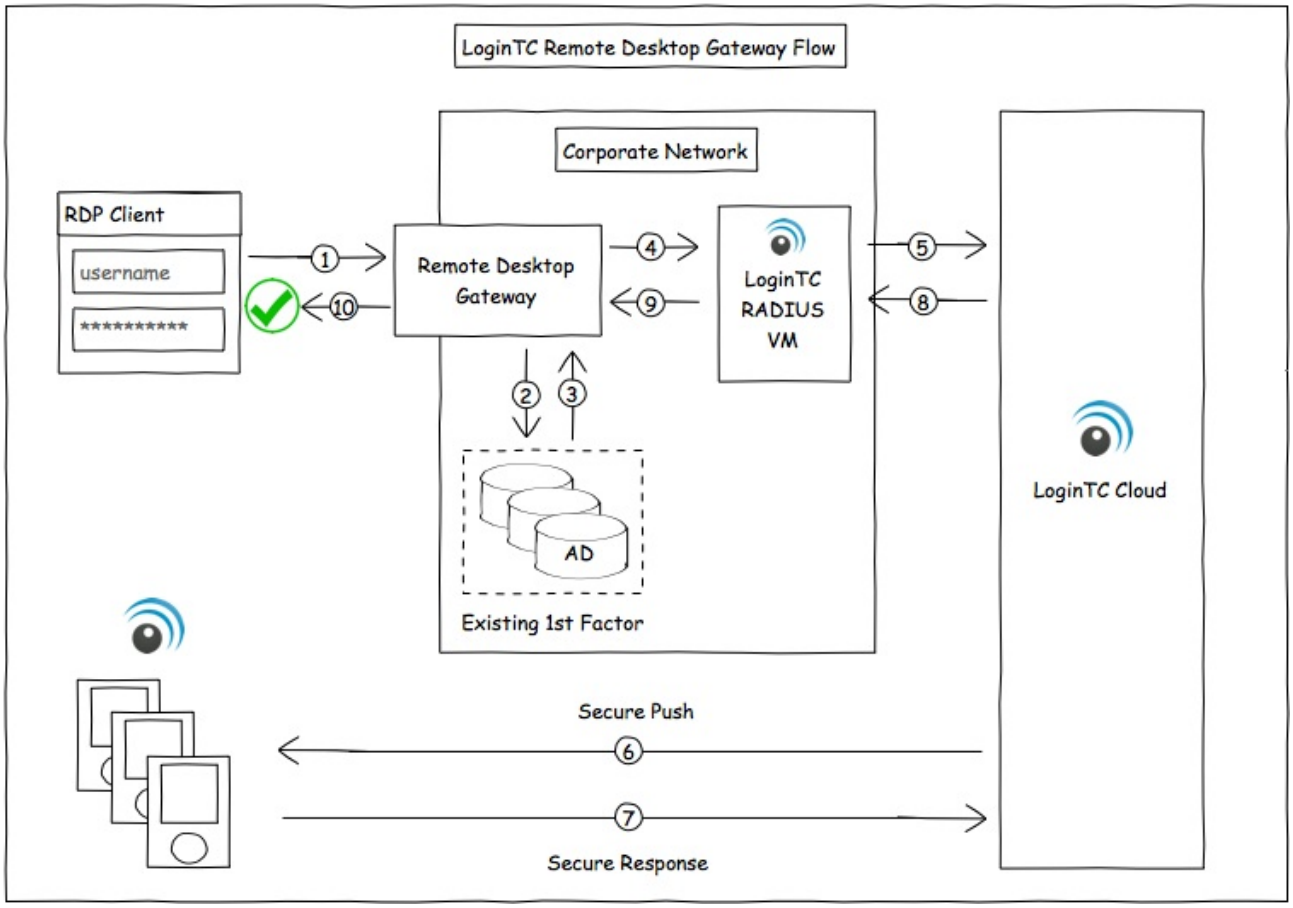
Overview

The LoginTC RD Gateway with RADIUS Connector protects access to your Microsoft Remote Desktop Gateway (RD Gateway) by adding a second factor LoginTC challenge to existing username and password authentication to your Remote Desktop resources.

This guide instructs you on how to configure your RD Gateway to use the LoginTC RADIUS Connector for two-factor authentication. If you would like to protect your RD Web Access then you may be interested in the: LoginTC RD Web Access Connector.

Note: Bypass Codes and OTPs not supported in this setup

As a result of how Microsoft implements using an external RADIUS authenticating server both bypass codes and OTPs are not supported for this setup. For bypass code and OTP support you may be interested in: LoginTC RD Web Access Connector



Architecture and Authentication Flow

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin account
- Microsoft Windows Server 2012 R2 running the RD Gateway role
- Computer virtualization software such as VMware ESXi, VirtualBox, or Hyper-V
- Virtual Machine requirements:
  - 1024 MiB RAM
  - 8 GiB disk size

Working Remote Desktop Gateway Deployment

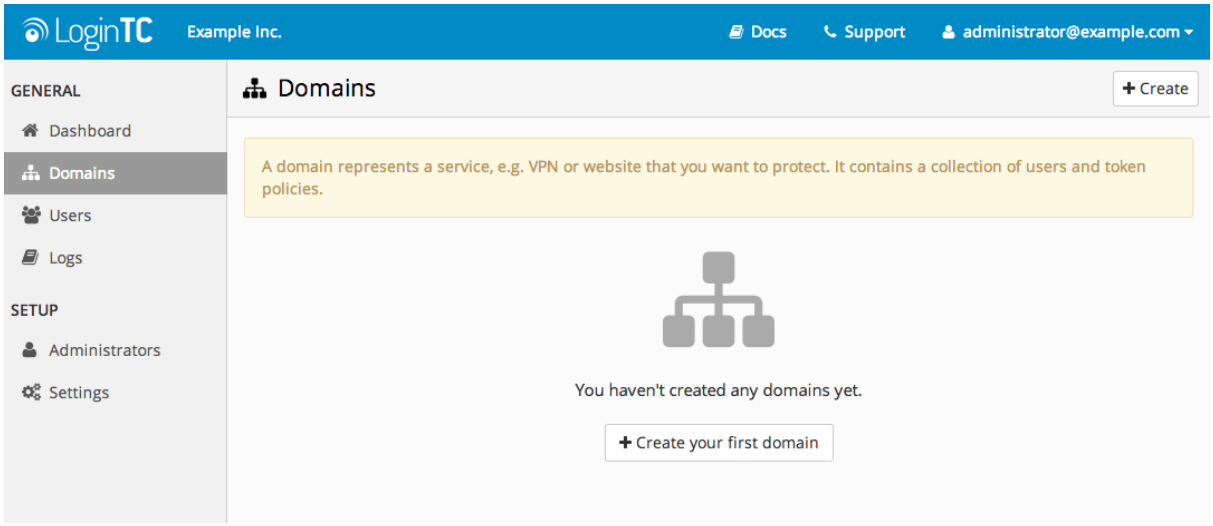
It is strongly recommended that you have a working and tested Remote Desktop Gateway deployment prior to adding LoginTC authentication.

RADIUS Domain Creation

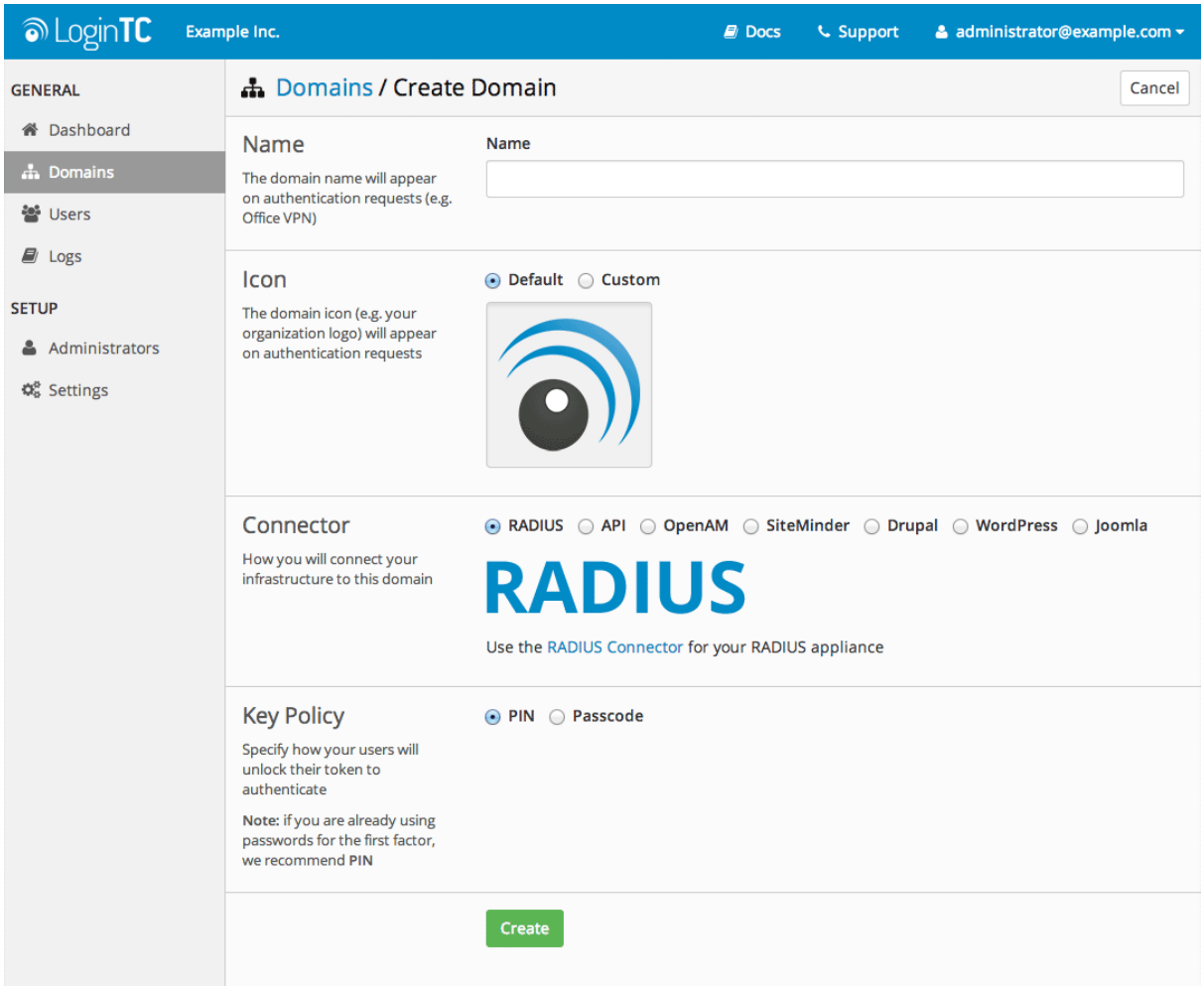
Create a RADIUS domain in LoginTC Admin. The domain represents a service (e.g. your RD Gateway) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

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**:



4. Enter domain information:



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.

RADIUS Connector Configuration

In this sectino you will be configuring the LoginTC RADIUS Connector virtual appliance to receive RADIUS requests.

1. LoginTC

This section describes how the appliance itself authenticates againstLoginTC 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 check. Since your RD Gateway will perform the first factor check, this will not be used on the LoginTC RADIUS Connector.

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 (i.e., your RD Gateway) will be connecting to the appliance and whether to encrypt API Key, password and secret parameters.

Data Encryption

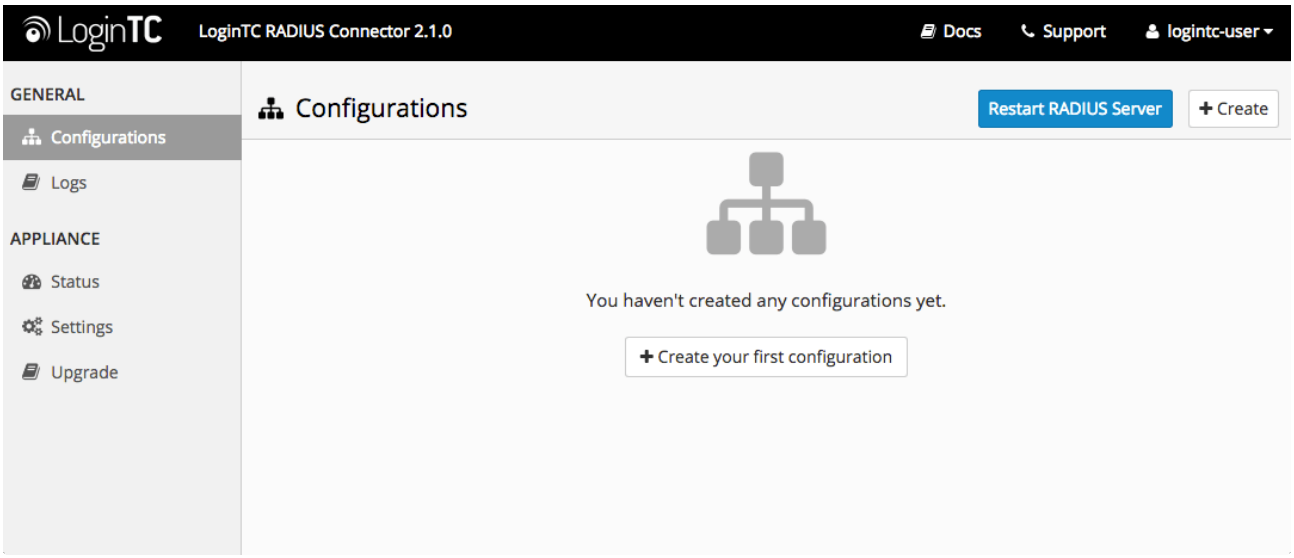
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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

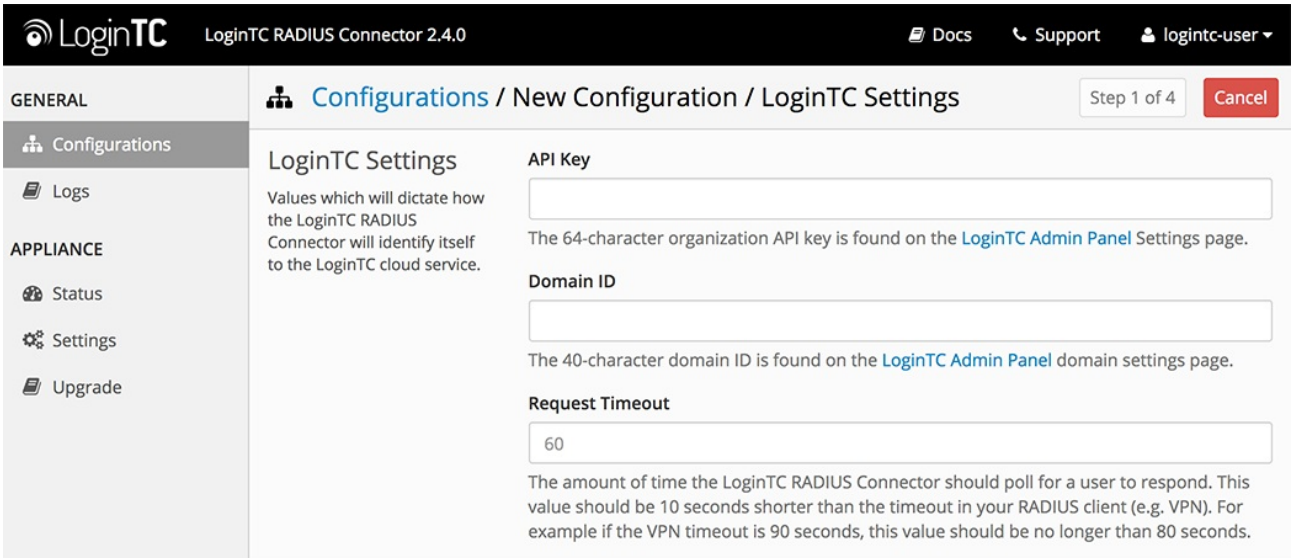
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



LoginTC Settings

Configure which LoginTC organization and domain to use:

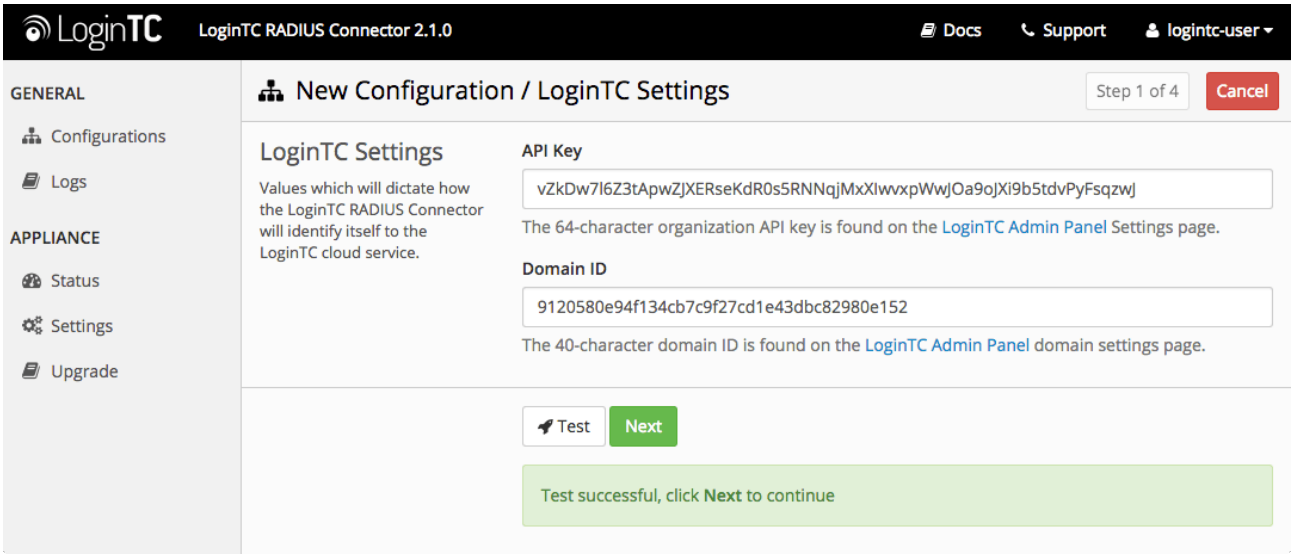


Configuration values:

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**:



First Authentication Factor

The LoginTC RADIUS Connector will not be performing the first factor authentication. Choose the **None** option and continue.

Passthrough

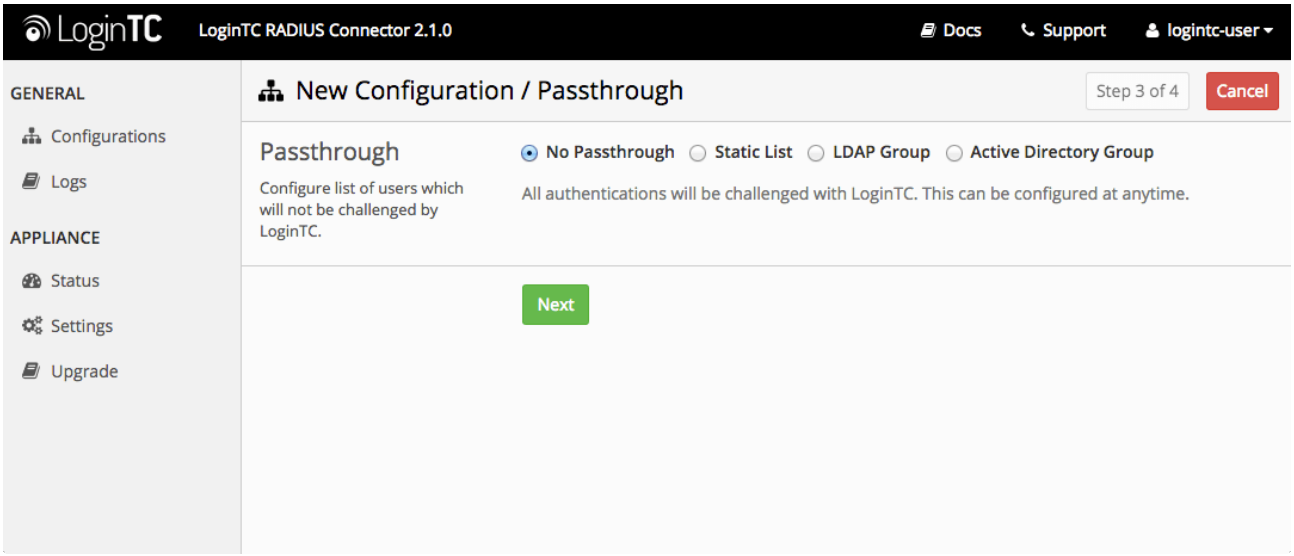
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.

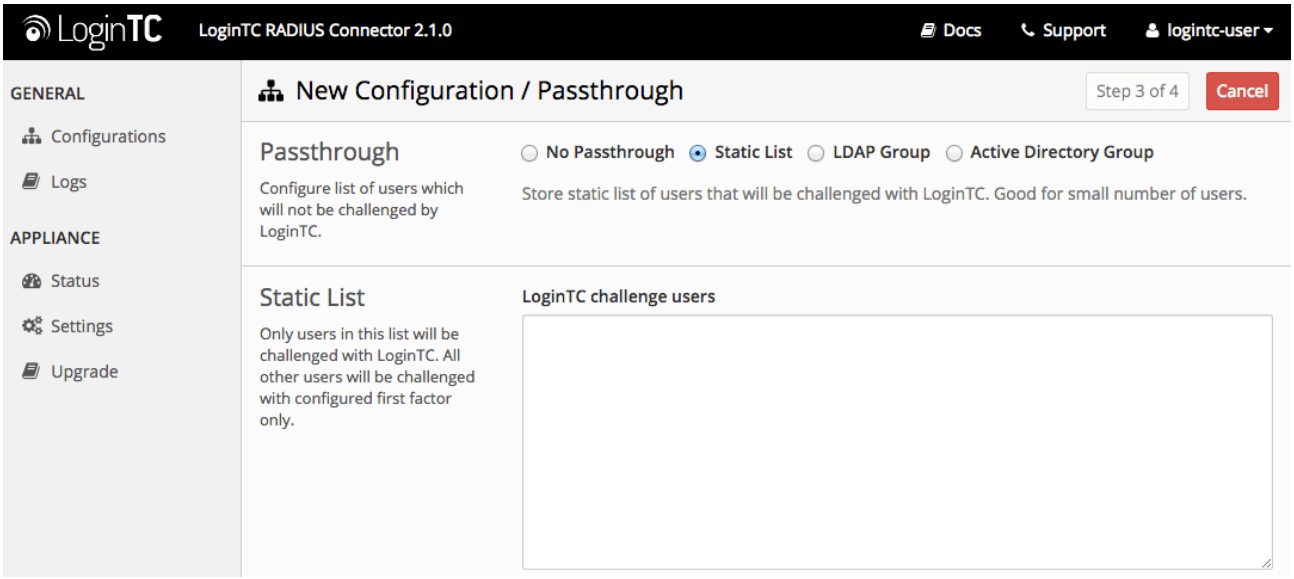
No Passthrough (default)

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



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.

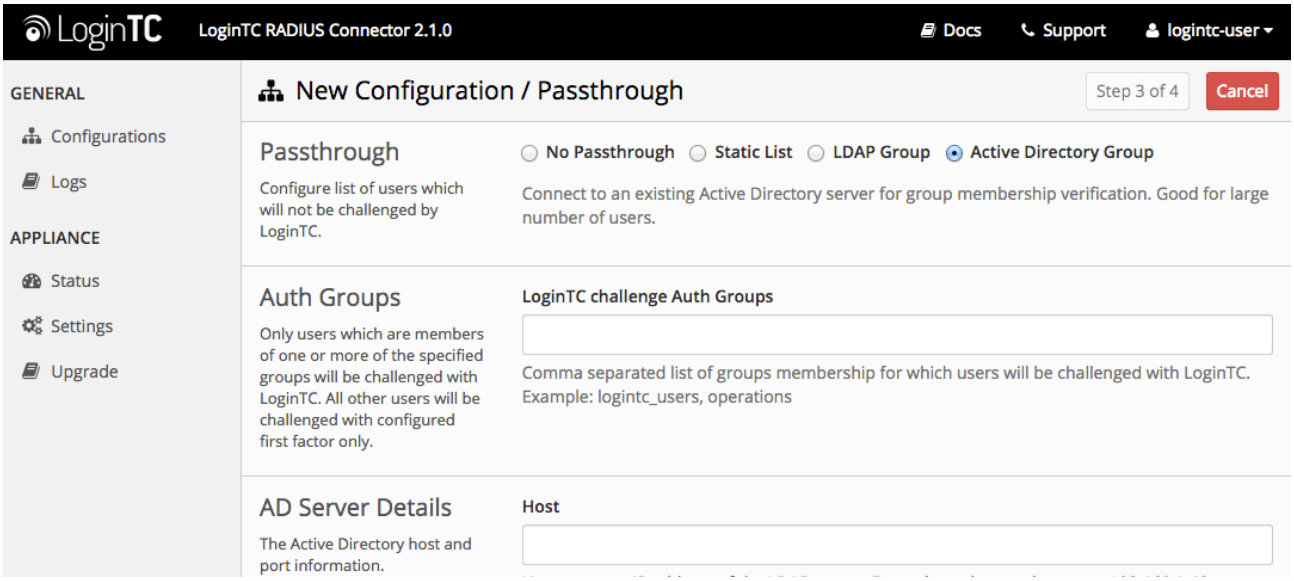


LoginTC challenge users: a new line separated list of usernames. For example:

```
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.



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

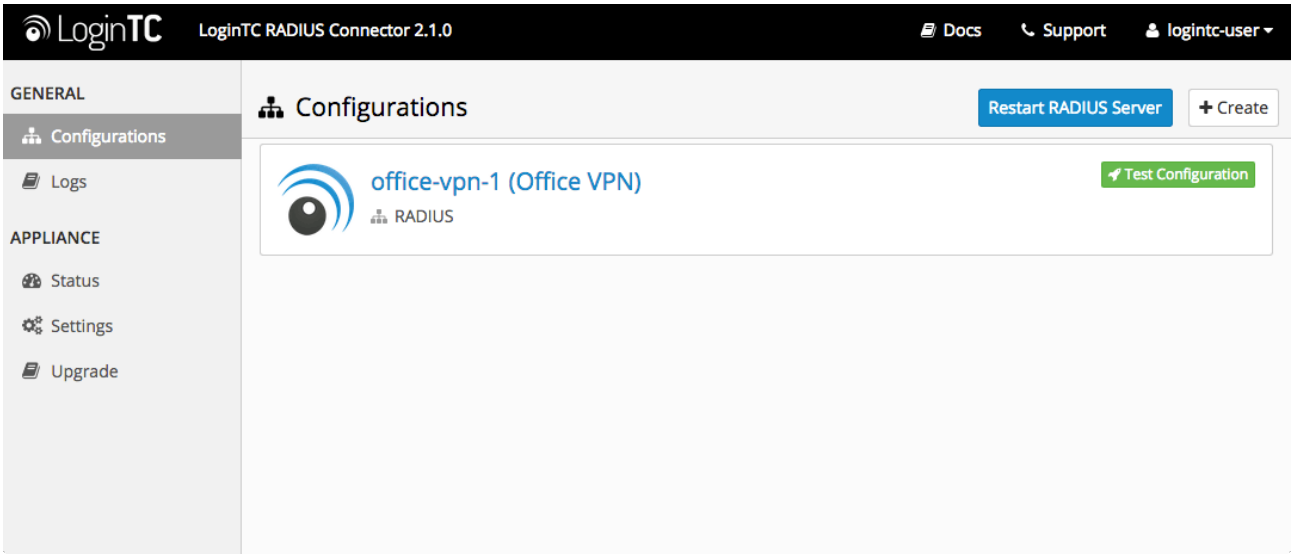
If Active Directory / LDAP Option was selected in First Authentication Factor the non-sensitive values will be pre-populated to avoid retyping and potential typos.

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

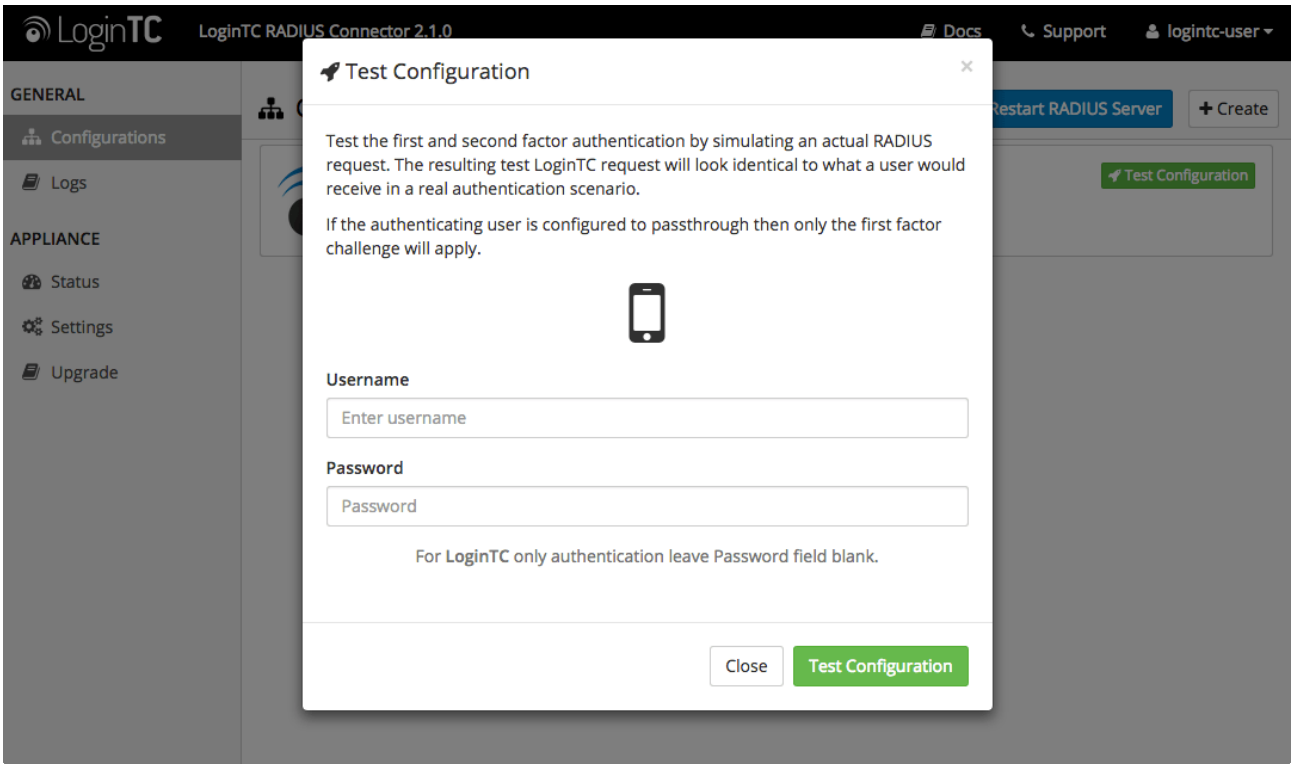
Testing

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:

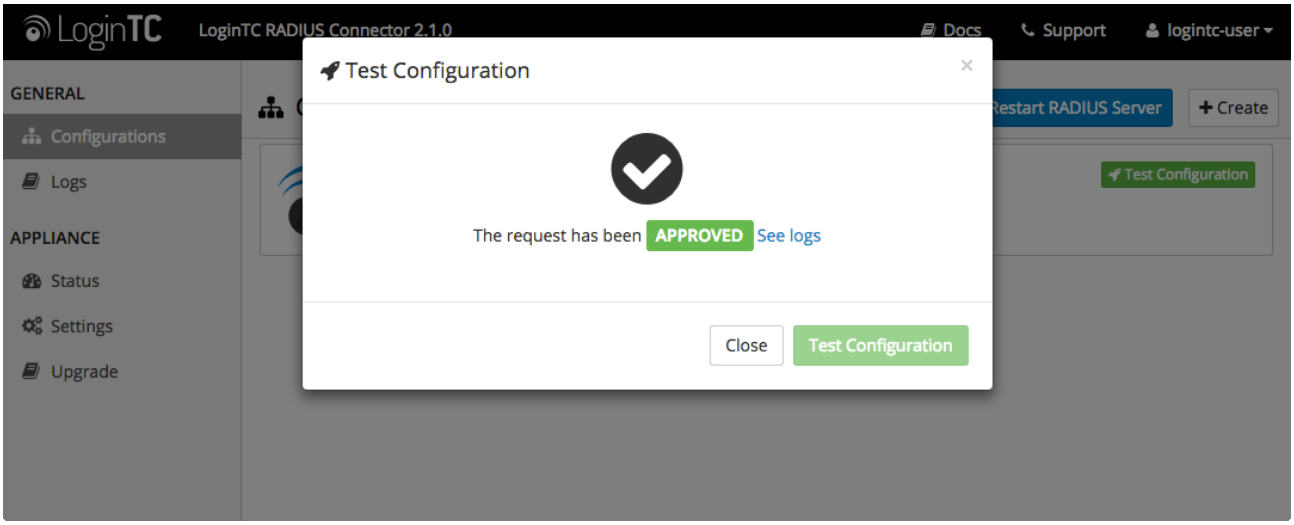
When you have loaded a token for your new user and domain, navigate to your appliance**web interface** URL:



Click **Test Configuration**:

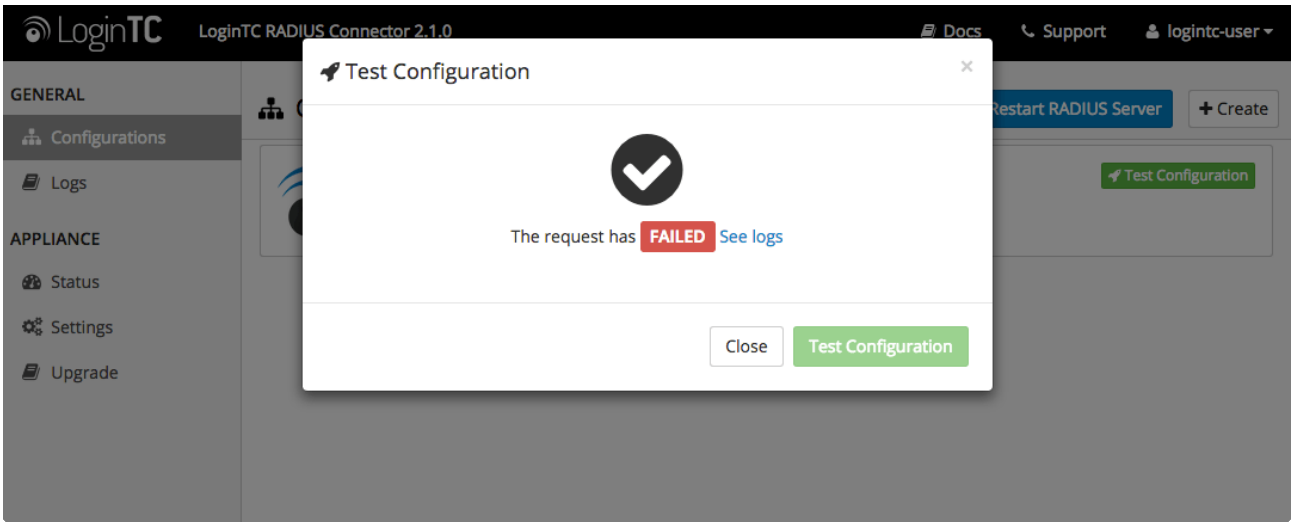


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

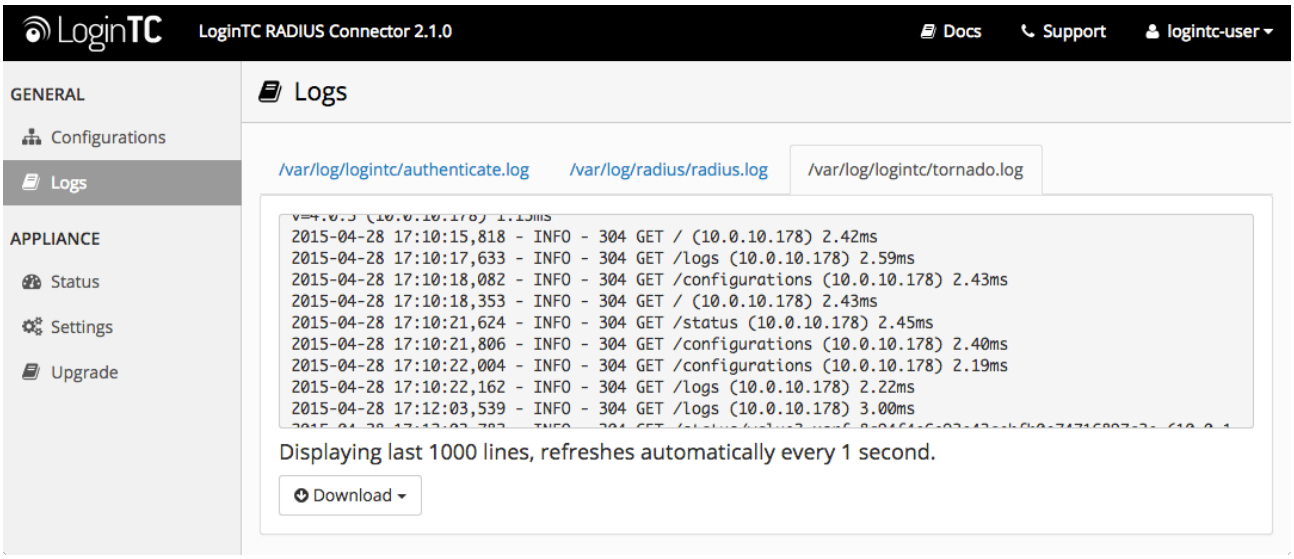


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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:



RD Gateway Configuration

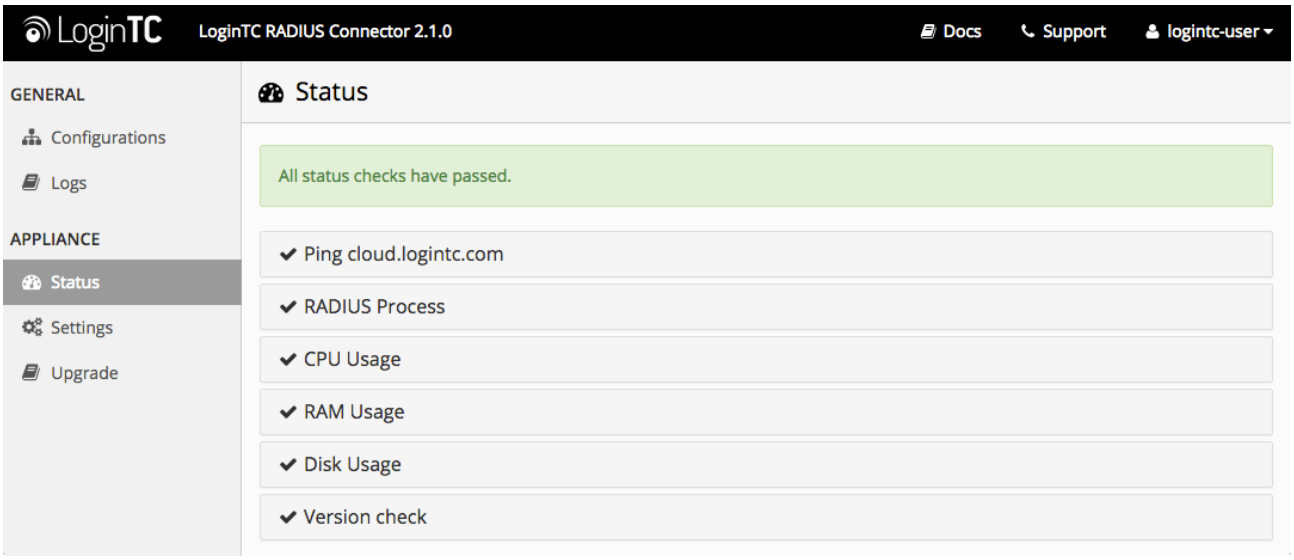
Once you have configured the LoginTC RADIUS Connector you will be able to configure your RD Gateway to use the LoginTC RADIUS Connector for second-factor authentication.

You may now test your RD Gateway.

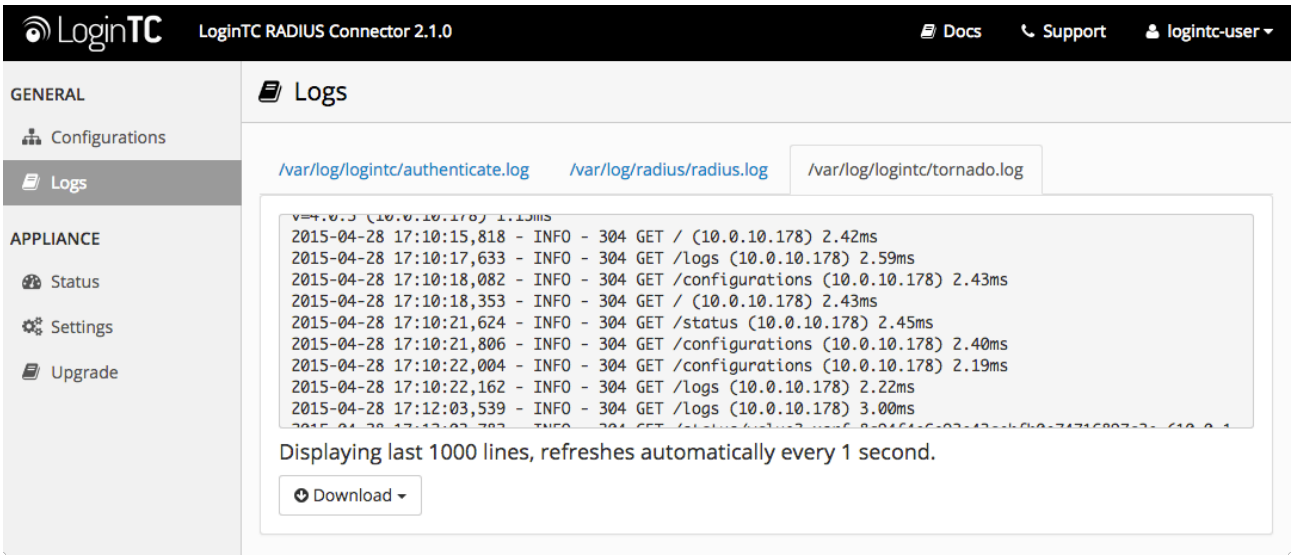
Troubleshooting

Not Authenticating

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



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



You may also find valuable information in the Microsoft **Event Viewer** under **Custom Views → ServerRoles → Network Policy and Access Services**

Email Support

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