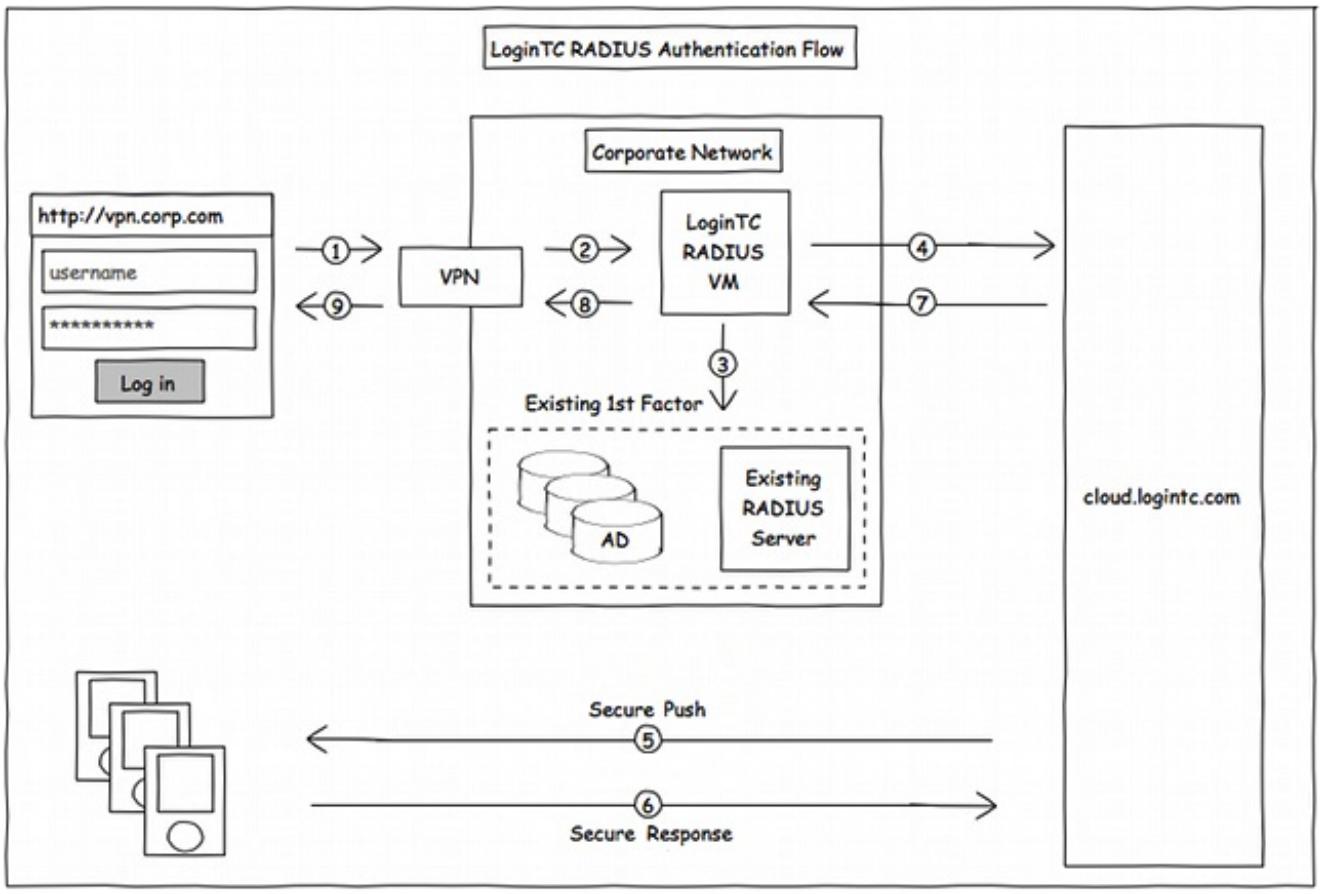
Two factor authentication for WatchGuard XTM and Firebox

logintc.com/docs/connectors/watchguard.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 WatchGuard to use LoginTC for the most secure two-factor authentication.



Compatibility

WatchGuard appliance compatibility:

- WatchGuard Firebox T10 Series
- WatchGuard XTM 2 Series
- WatchGuard XTM 3 Series
- WatchGuard XTM 5 Series
- WatchGuard Unified Threat Management (UTM)
- WatchGuard Next-Generation Firewall (NGFW)

- WatchGuard appliance supporting RADIUS authentication

Compatibility Guide

WatchGuard XTM, Firebox and any other appliance which have configurable RADIUS authentication are supported.

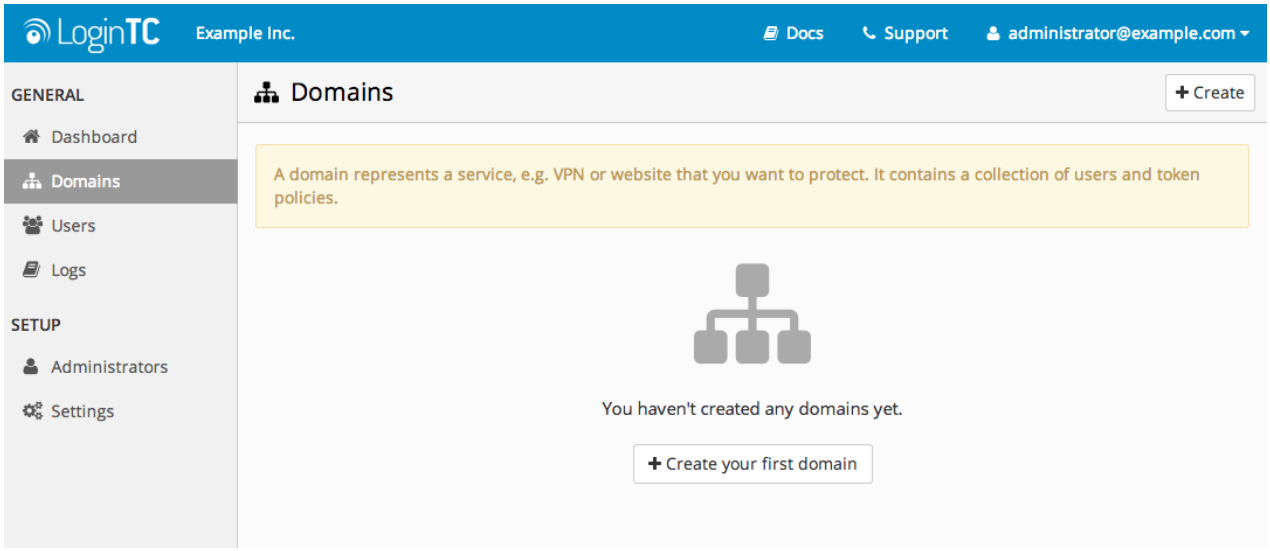
Prerequisites

Before proceeding, please ensure you have the following:

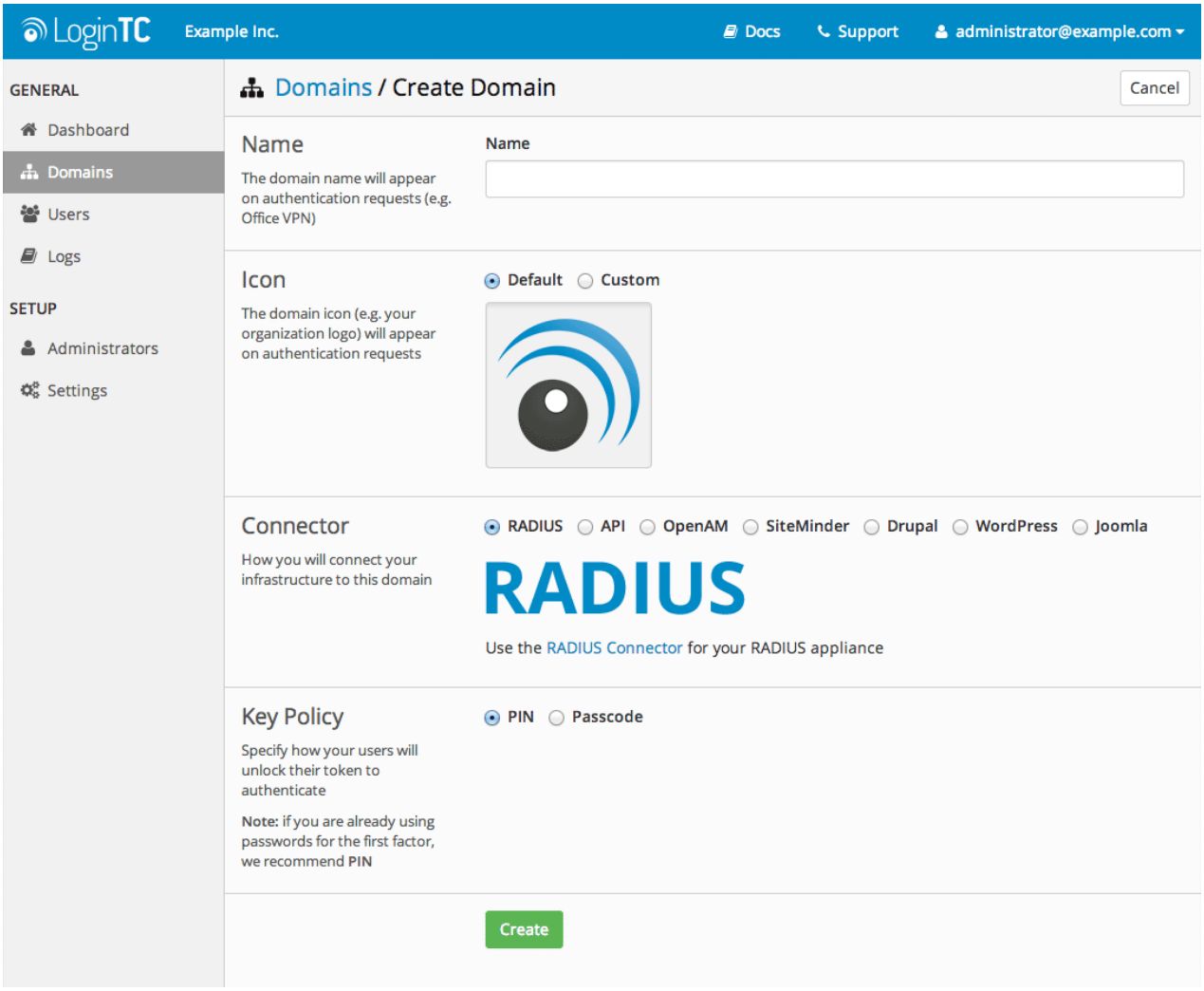
RADIUS Domain Creation

If you have already created a LoginTC 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:



Name

Choose a name to identify your LoginTC 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` can run `sudo su` to become the `root` user.

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

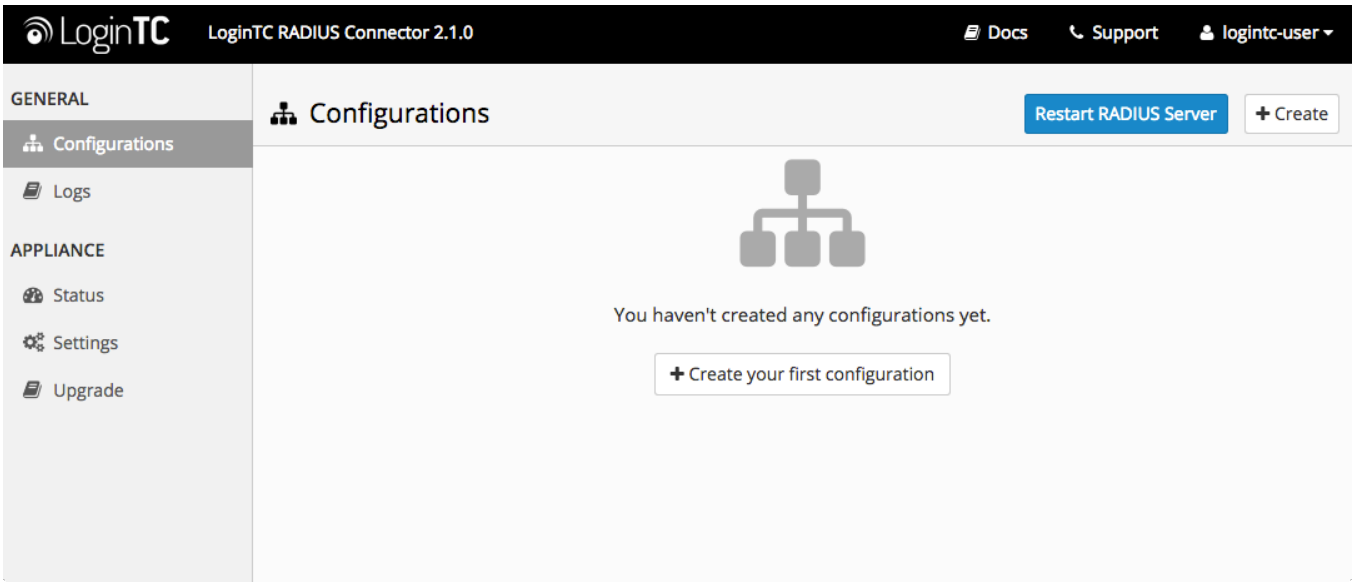
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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

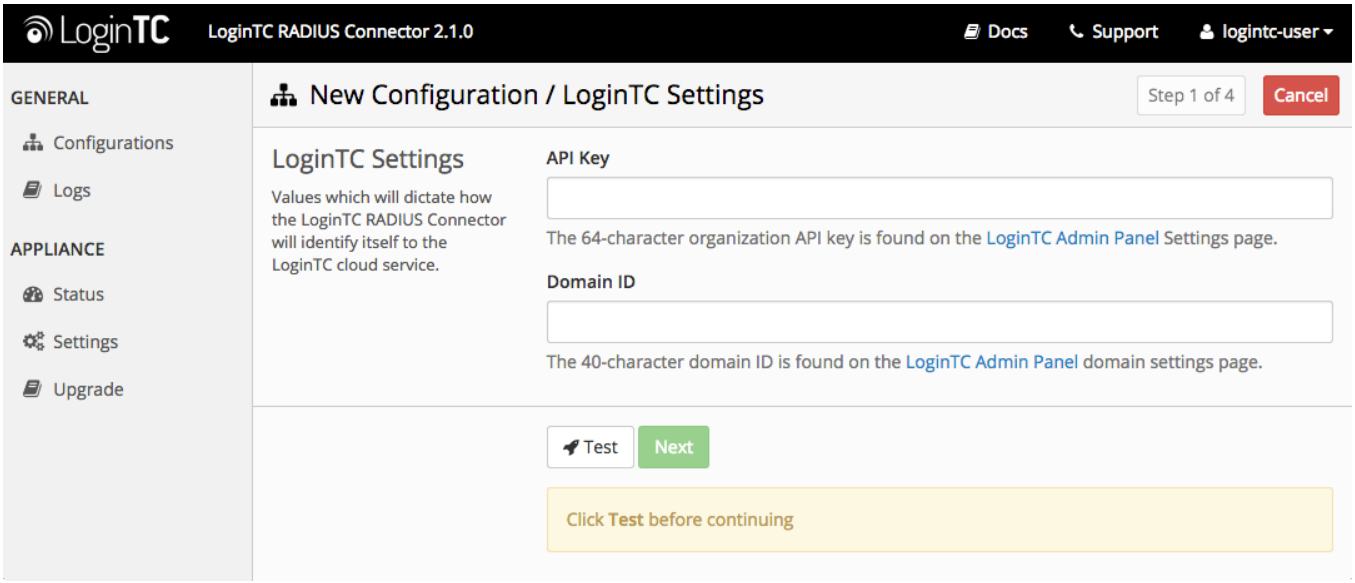
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



LoginTC Settings

Configure which LoginTC organization and domain to use:

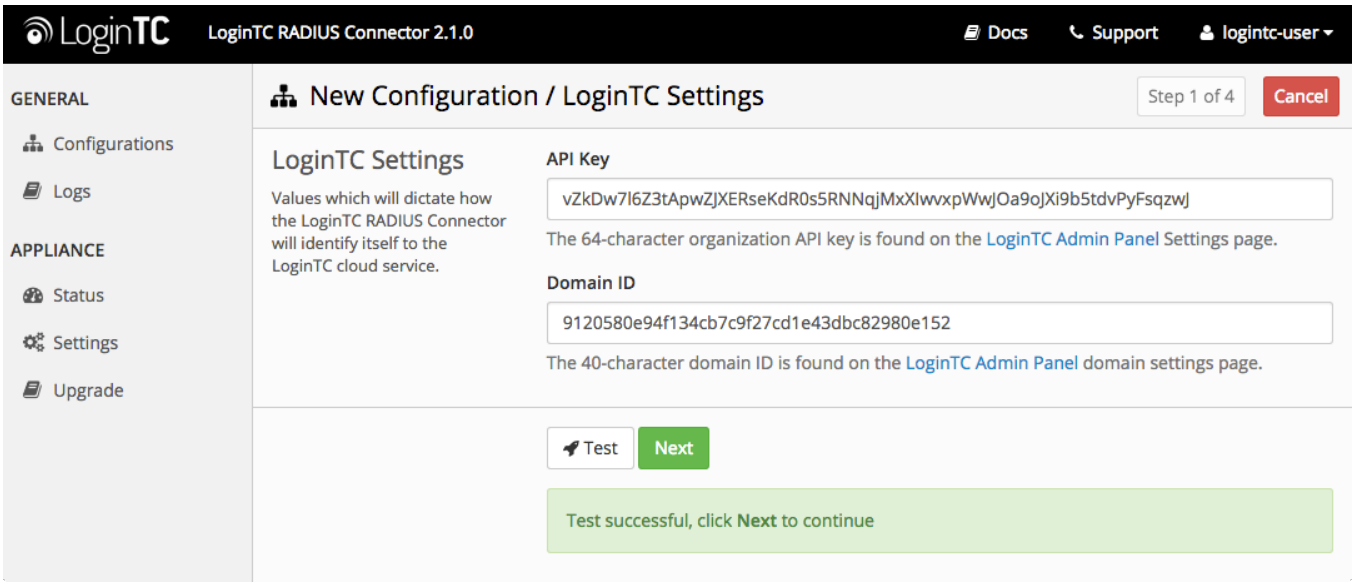


Configuration values:

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

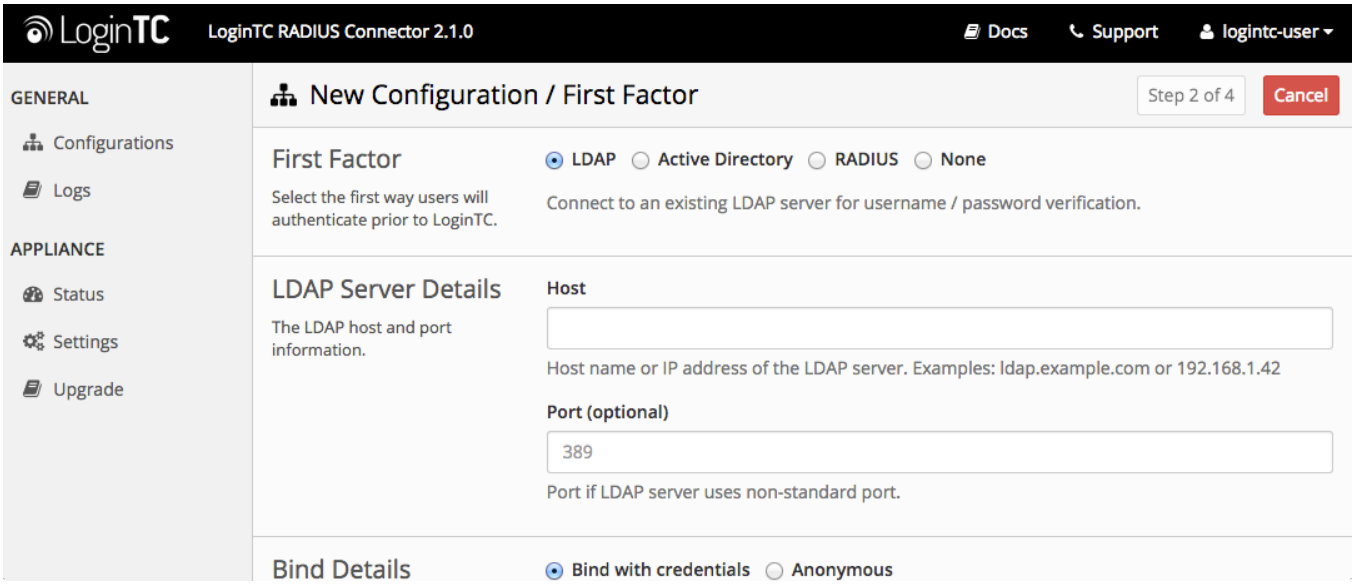
The API key is found on the LoginTC Admin Settings page. The Domain ID is found on your domain settings page.

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



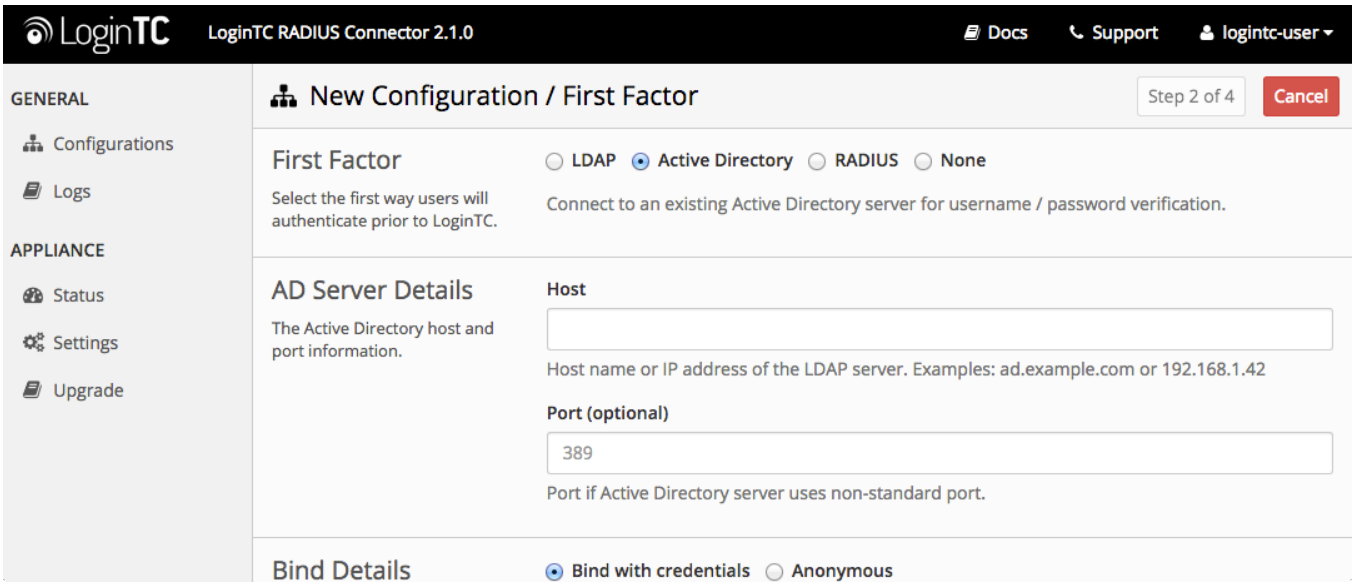
First Authentication Factor

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.



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**:



Configuration values:

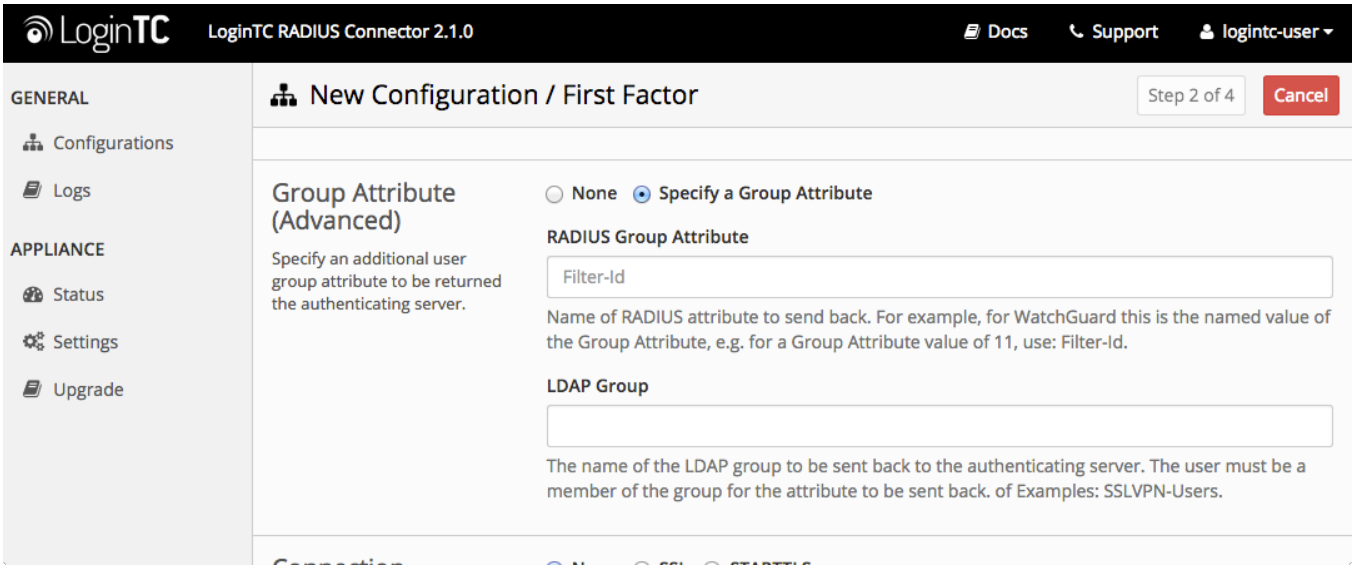
`host`	Host or IP address of the LDAP server	`ldap.example.com`, `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389`/`636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The password for the above bind_dn account	`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`, `uid`
`attr_name`	The attribute containing the user's real name	`displayName`, `cn`
`attr_email`	The attribute containing the user's email address	`mail`, `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`, `startTLS`

`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`
`cert` (optional)	Certificate file (PEM format)	`/opt/logintc/cert.pem`
`key` (optional)	Key file (PEM format)	`/opt/logintc/key.pem`

Group Attribute and Access Control

WatchGuard devices can use the **Group Attribute** value to set the attribute that carries the User Group information. This information is used for access control. Configure `Group Attribute` in Active Directory / LDAP Option to include the Filter ID string with the user authentication message that gets sent to the Watchguard device.

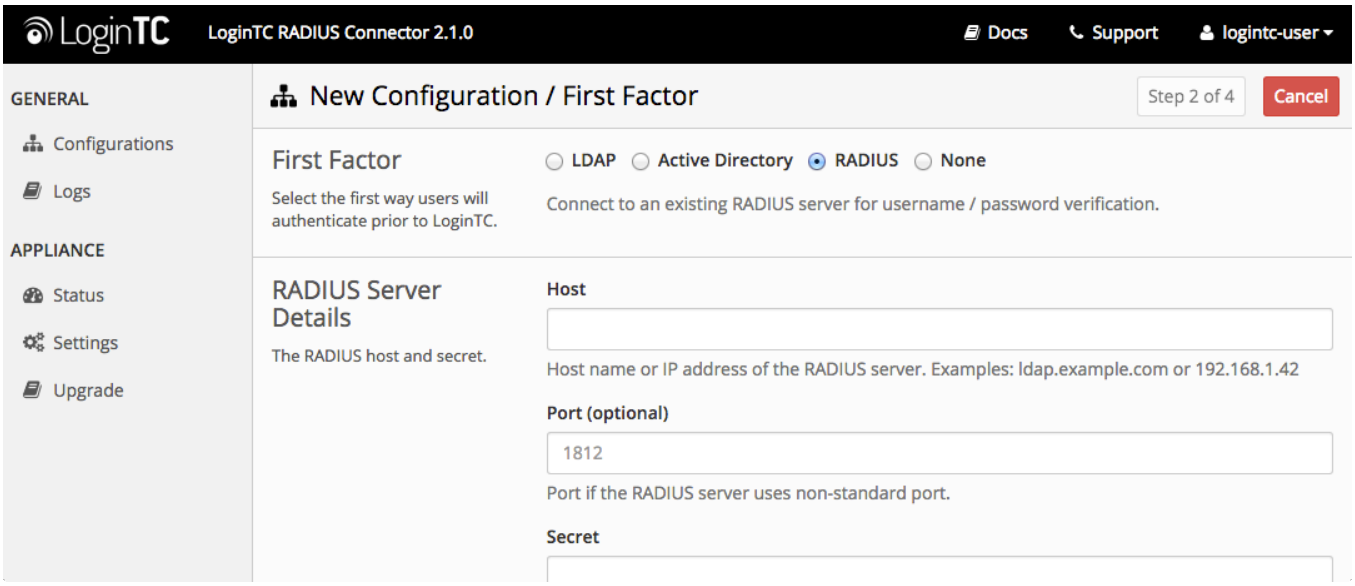
For example set `RADIUS Group Attribute` to `Filter-Id` and `LDAP Group` to `engineerGroup` or `financeGroup`.



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:

`host`	Host or IP address of the RADIUS server	`radius.example.com`, `192.168.1.43`
`port` (optional)	Port if the RADIUS server uses non-standard (i.e., `1812`)	`6812`
`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

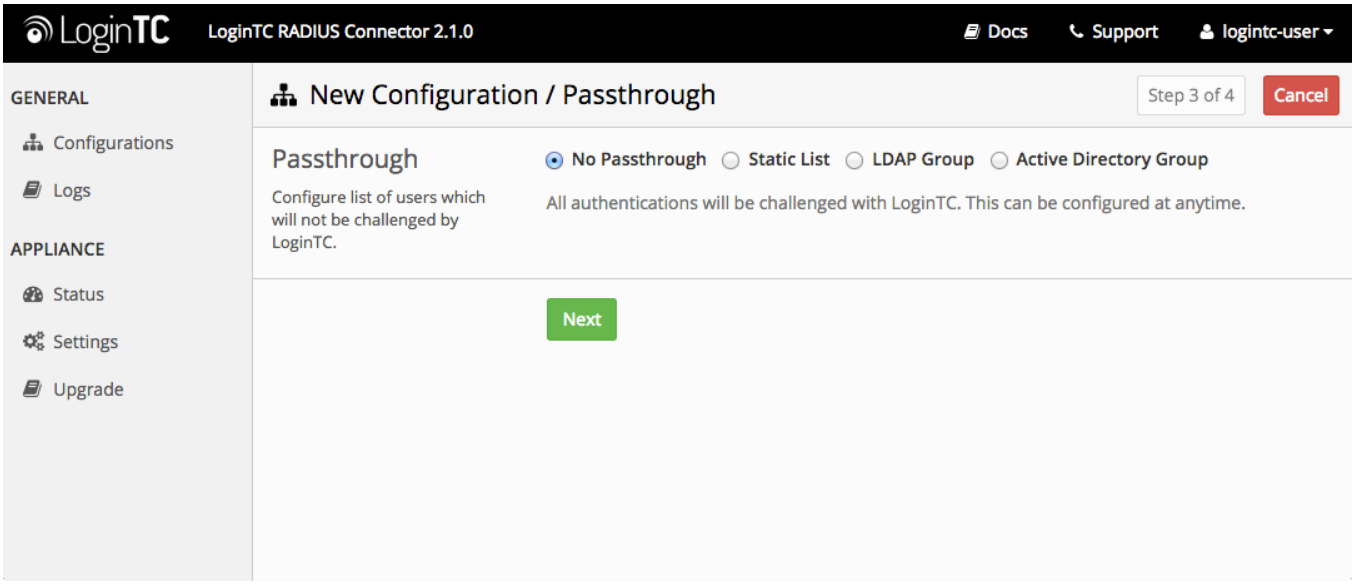
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.

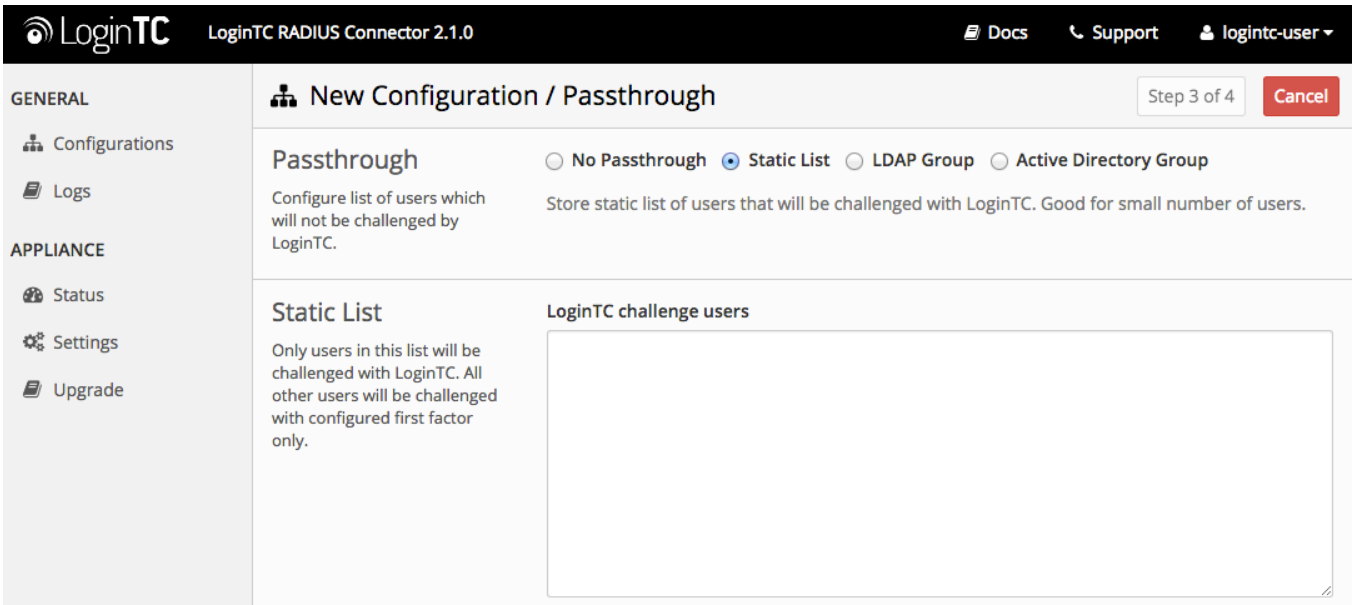
No Passthrough (default)

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



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.

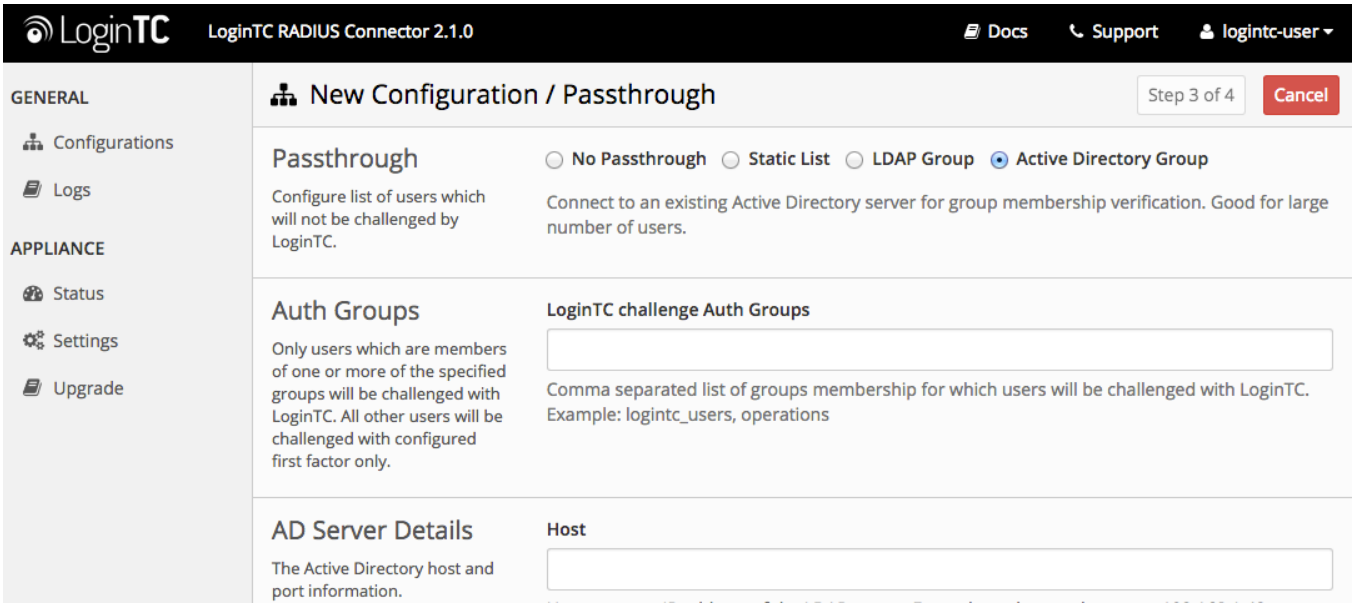


LoginTC challenge users: a new line separated list of usernames. For example:

```
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:

`LoginTC challenge auth groups`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users`, `two-factor-users`
`host`	Host or IP address of the LDAP server	`ldap.example.com`, `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`, `uid`
`attr_name`	The attribute containing the user's real name	`displayName`, `cn`
`attr_email`	The attribute containing the user's email address	`mail`, `email`
`encryption` (optional)	Encryption mechanism	`ssl`, `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

`cert` (optional)	Certificate file (PEM format)	`/opt/logintc/cert.pem`
`key` (optional)	Key file (PEM format)	`/opt/logintc/key.pem`

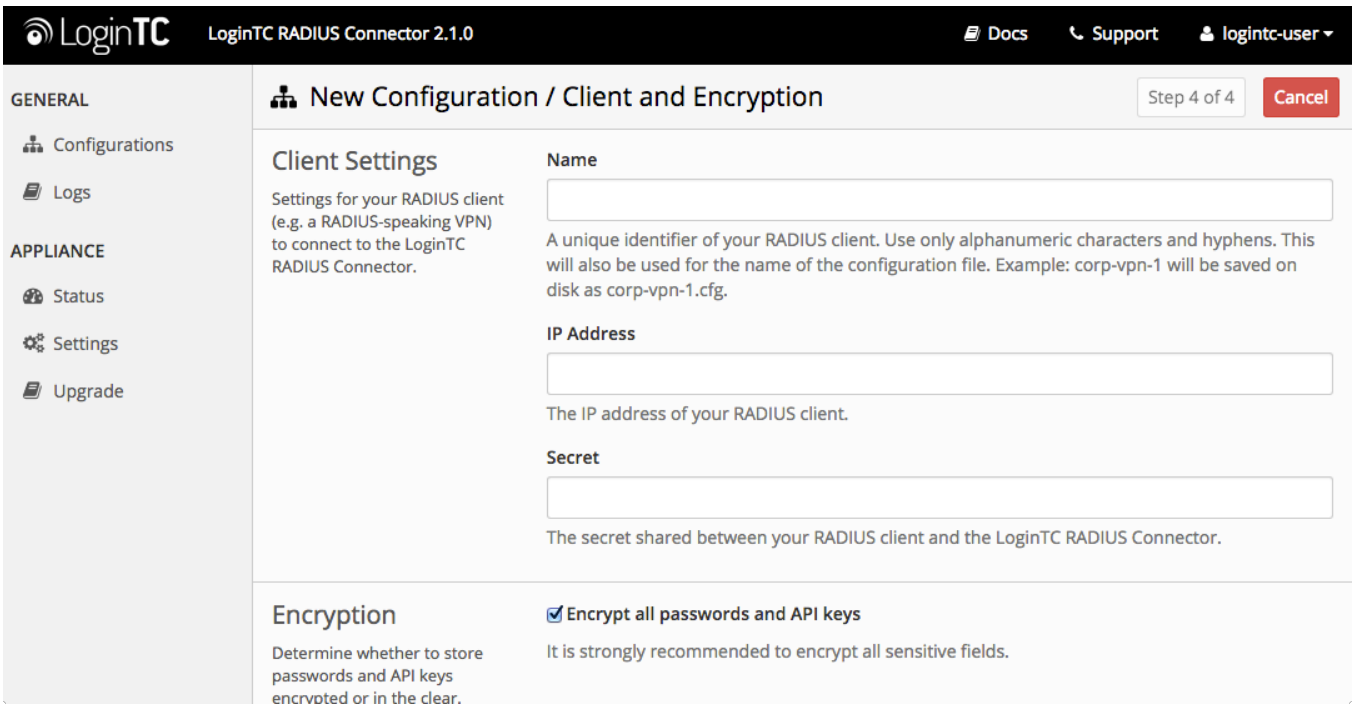
Configuration Simplified

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):



Client configuration values:

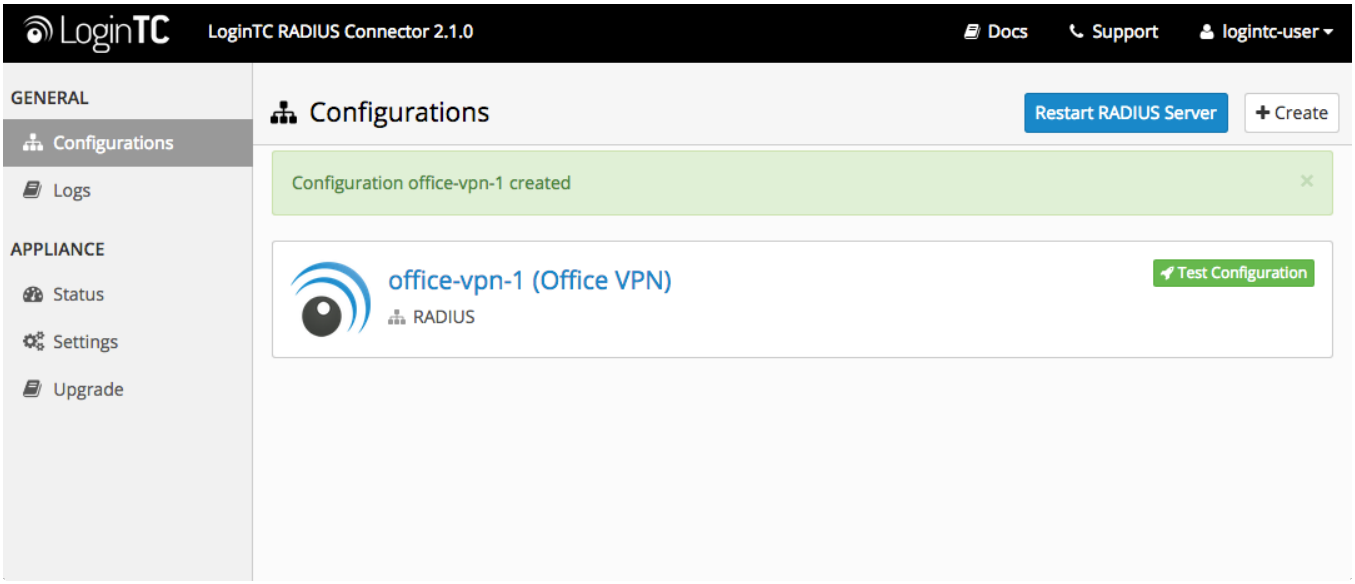
`name`	A unique identifier of your RADIUS client	`CorporateVPN`
`ip`	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	`192.168.1.44`
`secret`	The secret shared between the LoginTC RADIUS Connector and its client	`bigsecret`
`authentication`	The authentication factors (comma-separated)	`ldap,logintc`, `radius,logintc`, or `logintc`

Data Encryption

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

general best practice.

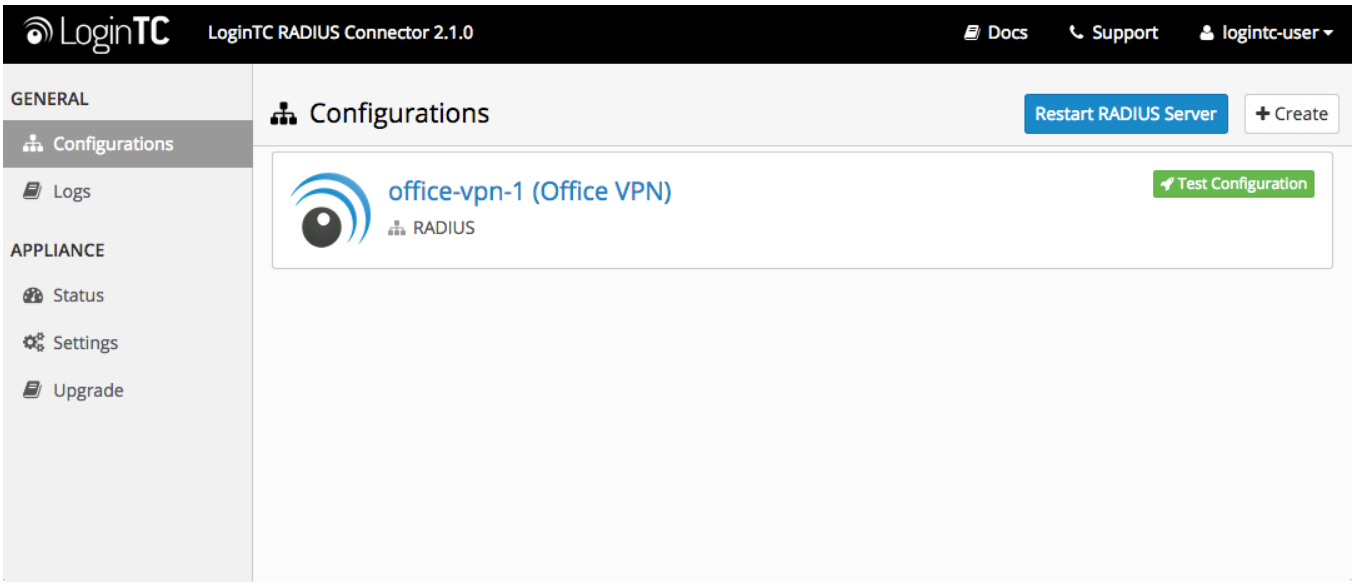
Click **Test** to validate the values and then click **Save**.



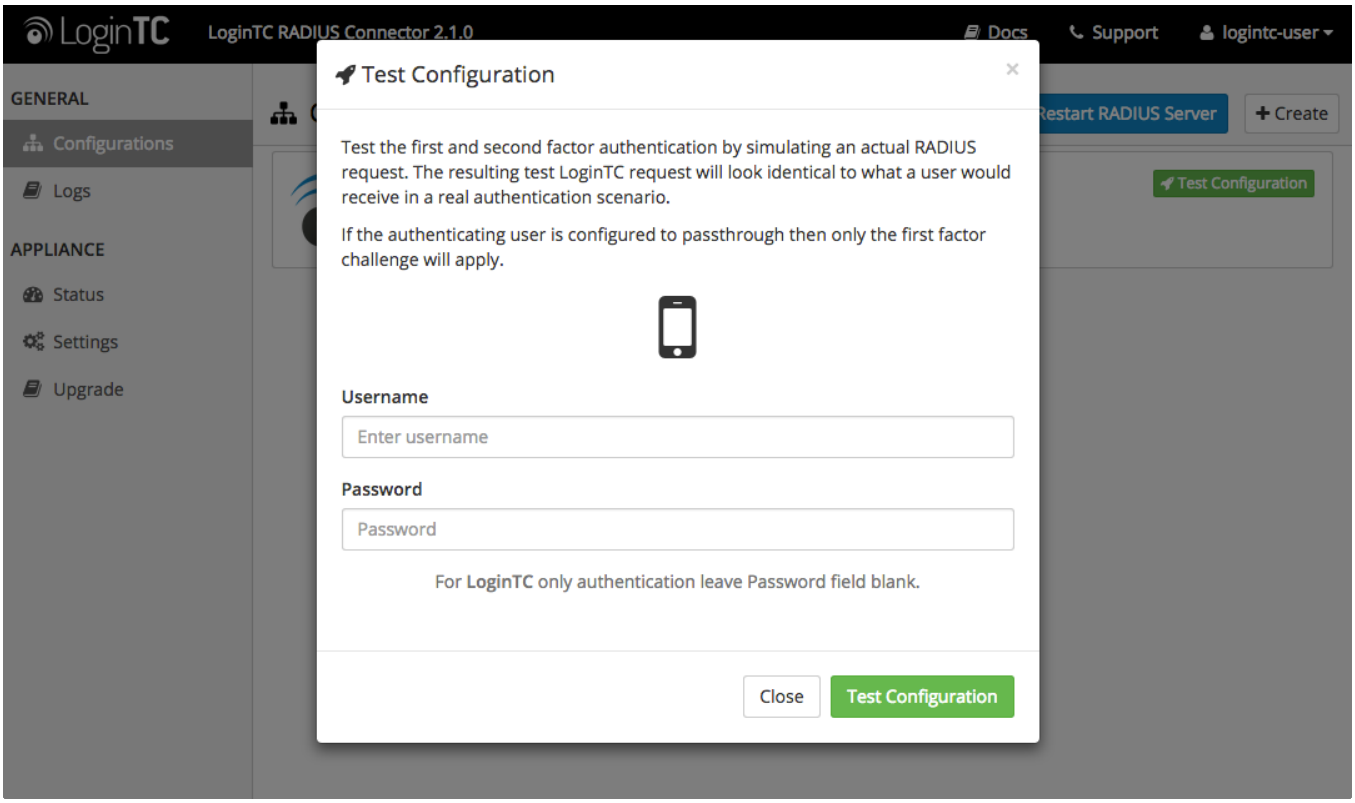
Testing

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:

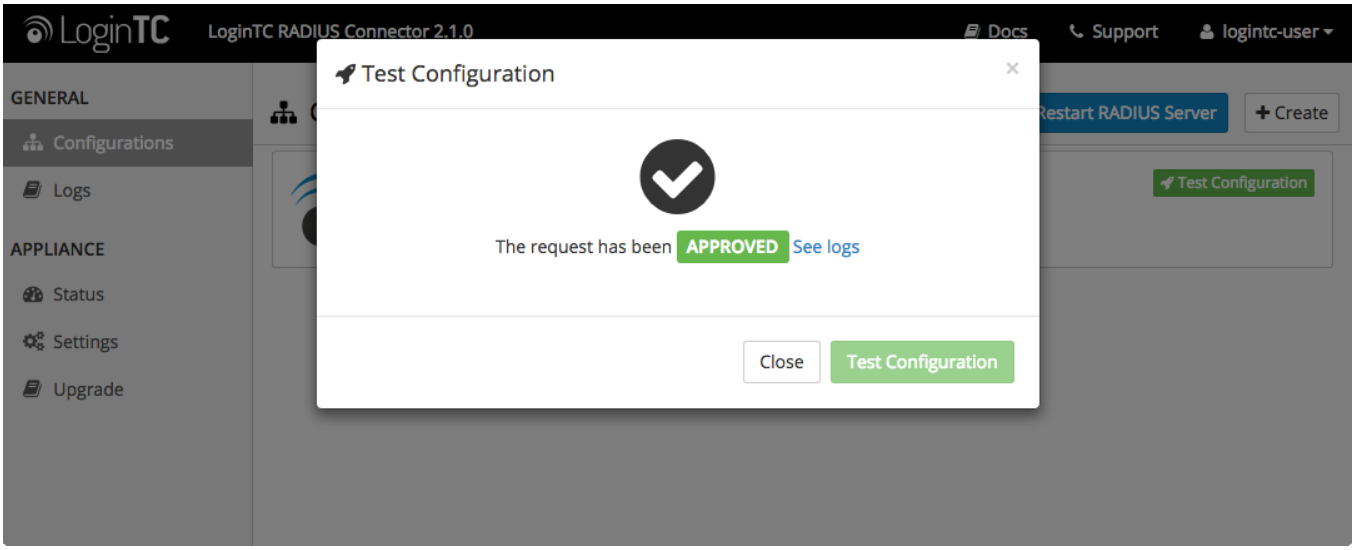
When you have loaded a token for your new user and domain, navigate to your appliance **web interface** URL:



Click **Test Configuration**:

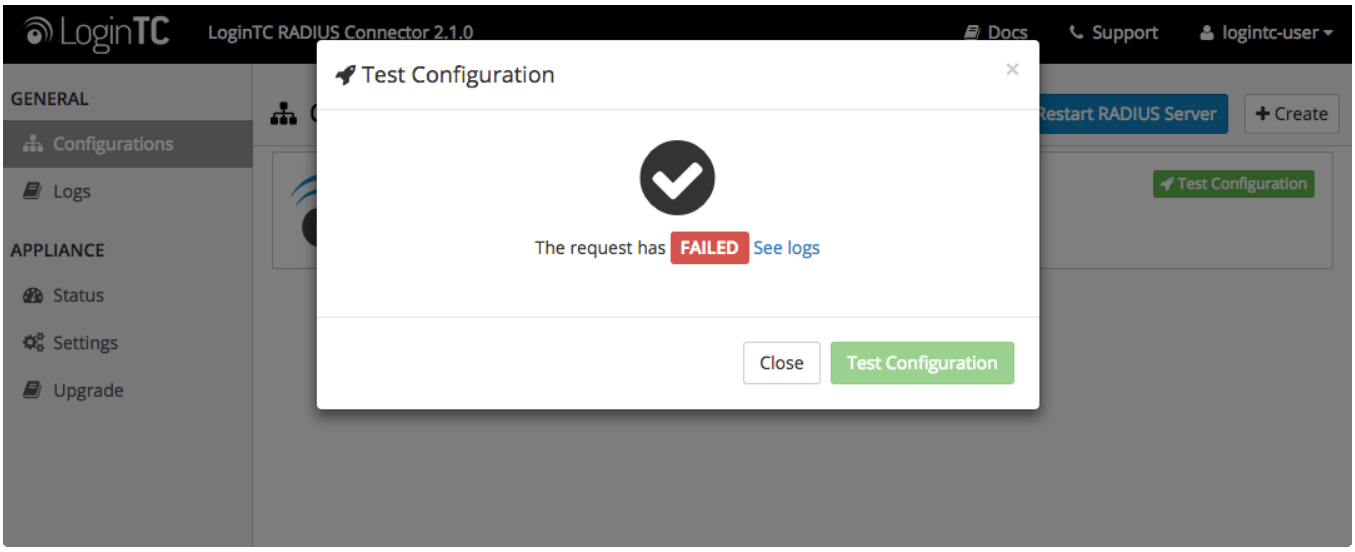


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

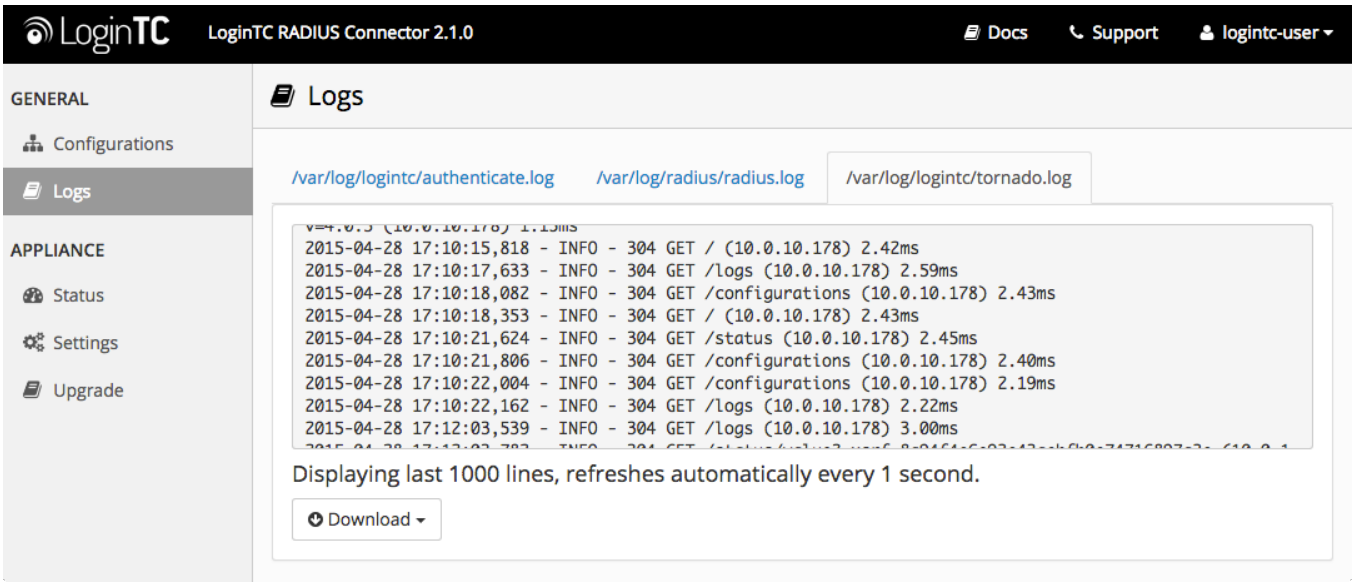


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



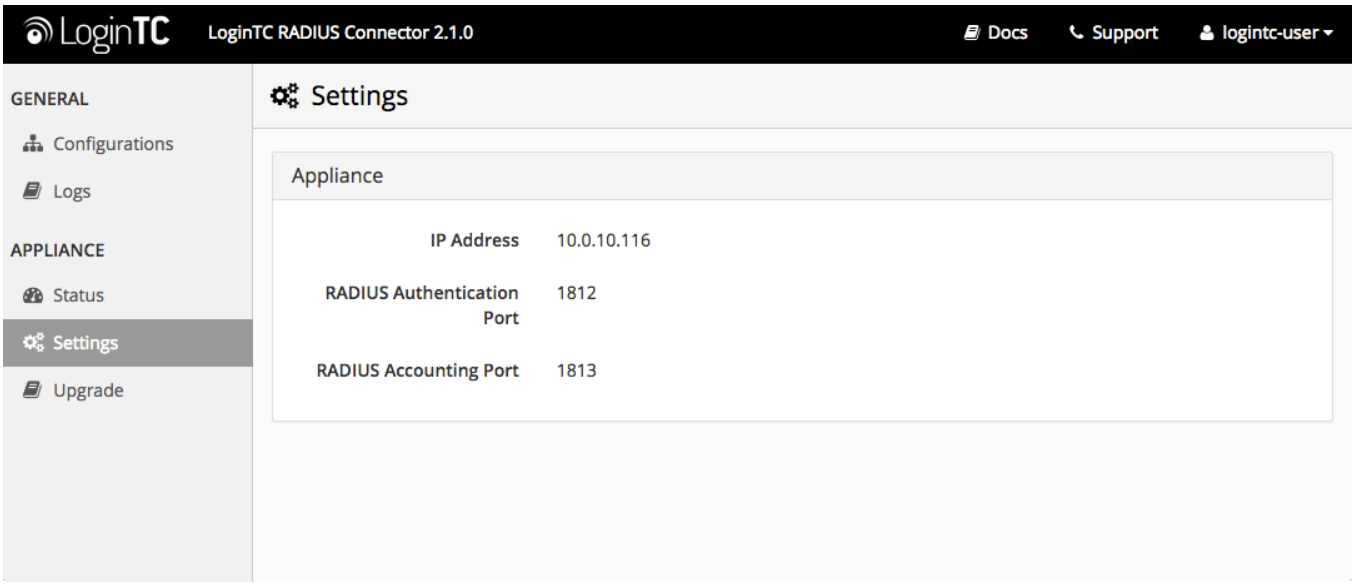
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:



WatchGuard Configuration - Quick Guide

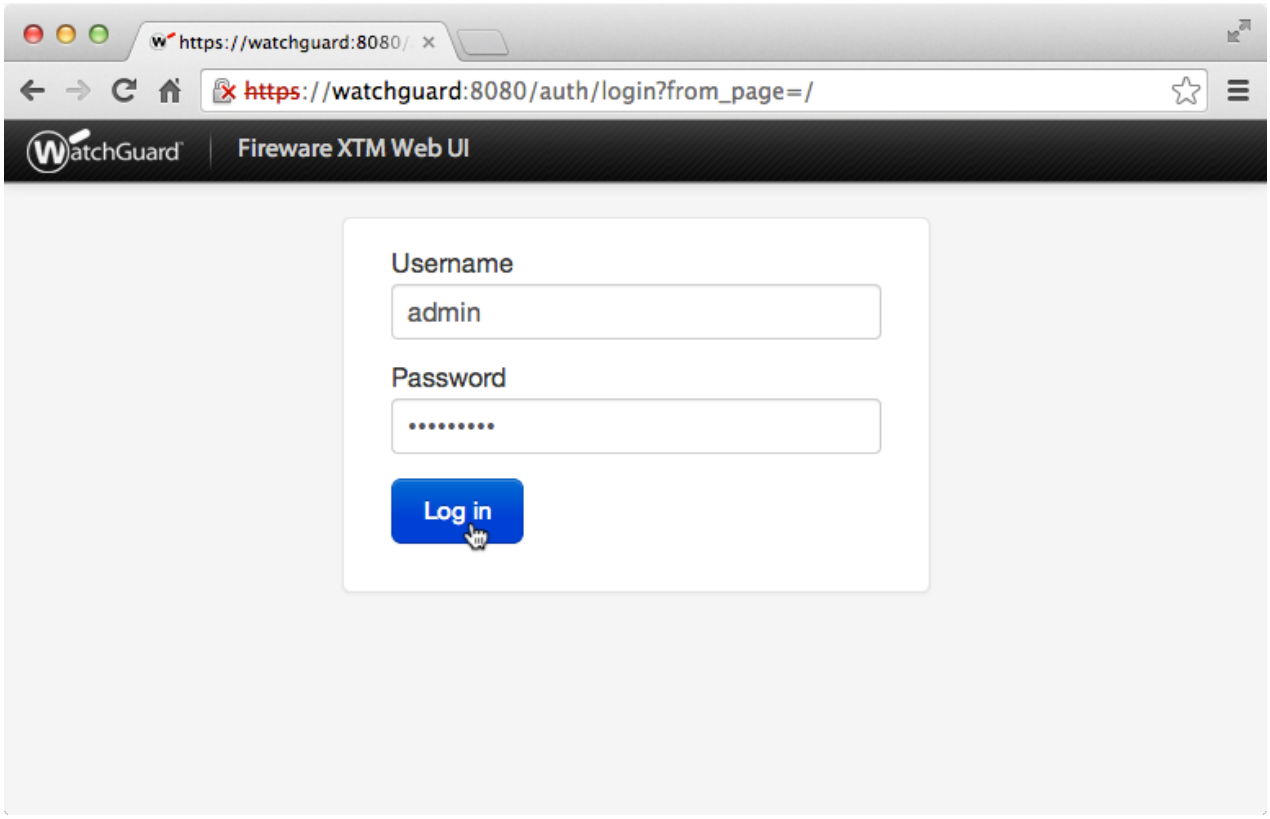
Once you are satisfied with your setup, configure your WatchGuard to use the LoginTC RADIUS Connector.

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

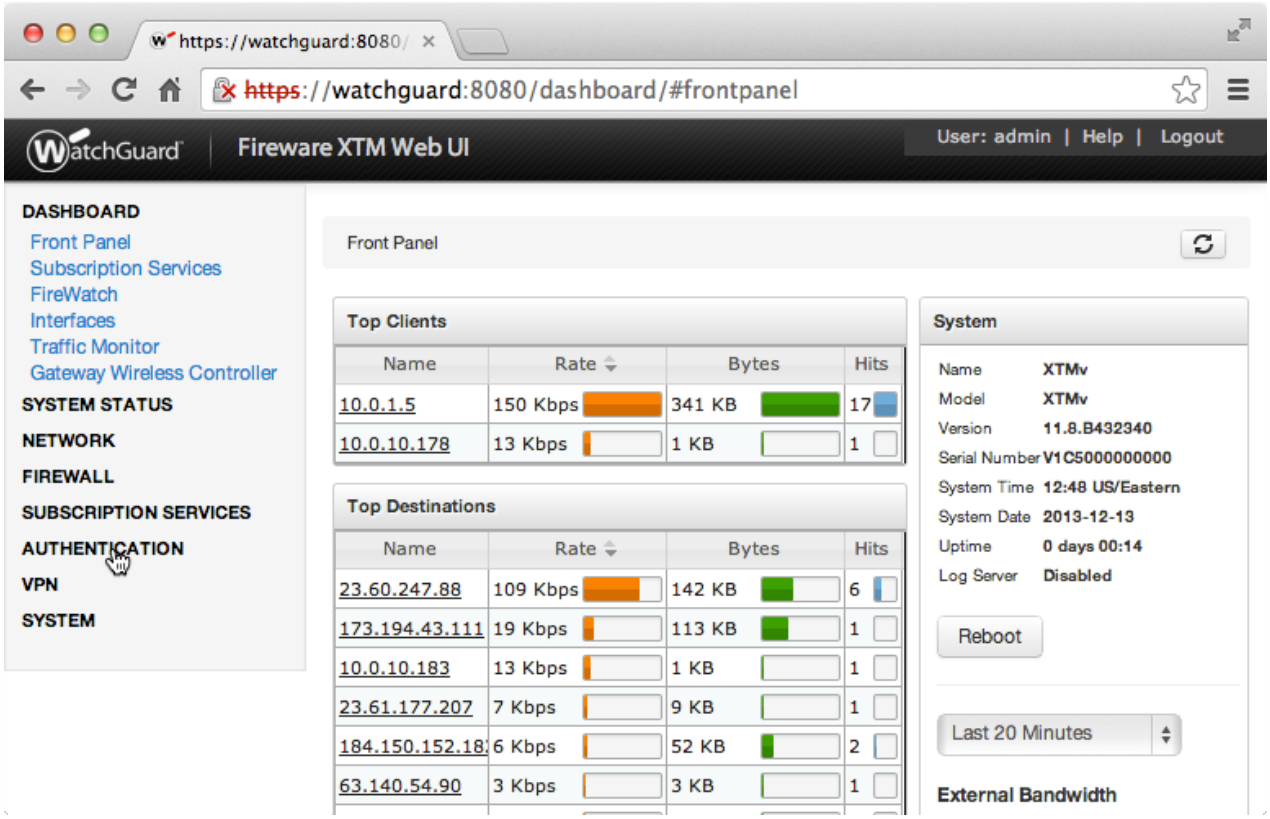


The following are quick steps to get VPN access protected with LoginTC. The instructions can be used for existing setups as well. Although these were performed on WatchGuard Fireware XTM Web UI using Mobile VPN with SSL, the same idea is true for the XTM series and other VPN connection types.

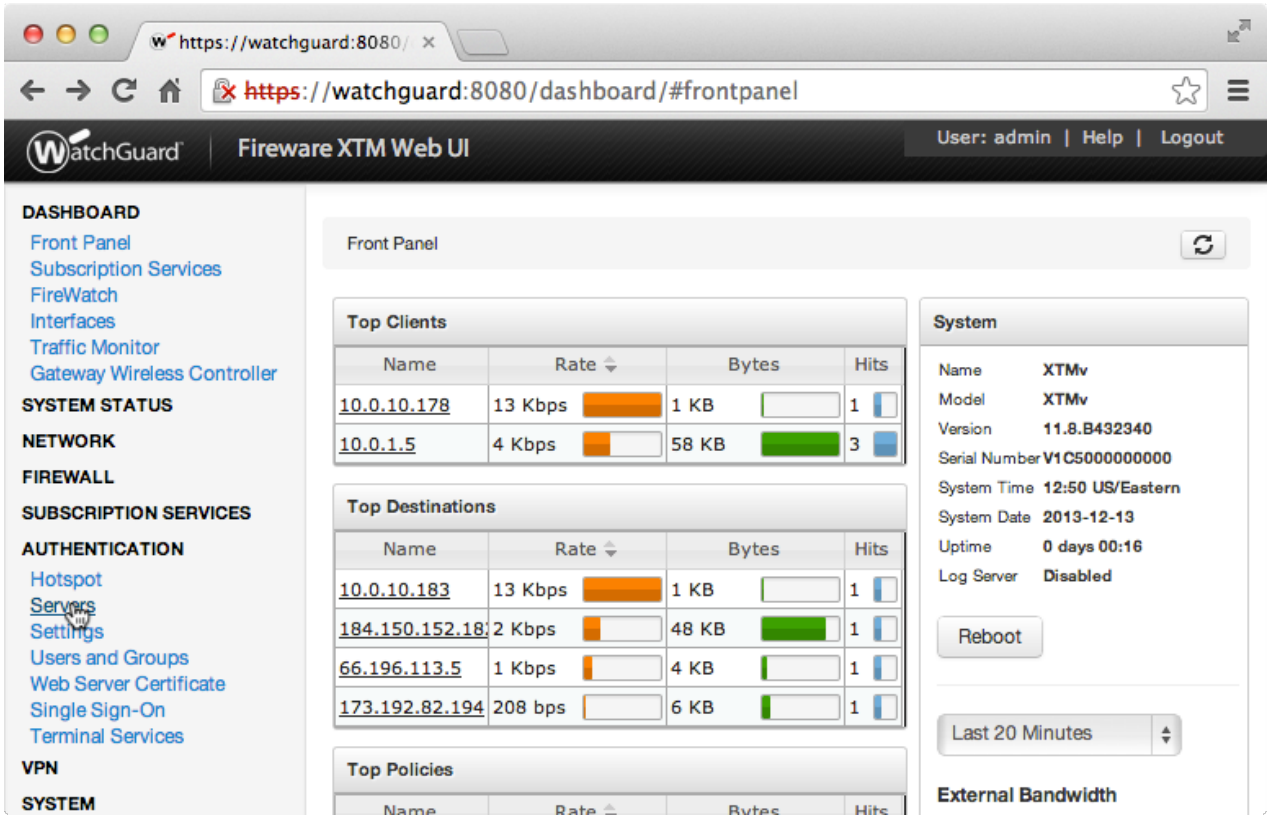
1. Log in to your WatchGuard (Fireware XTM Web UI)



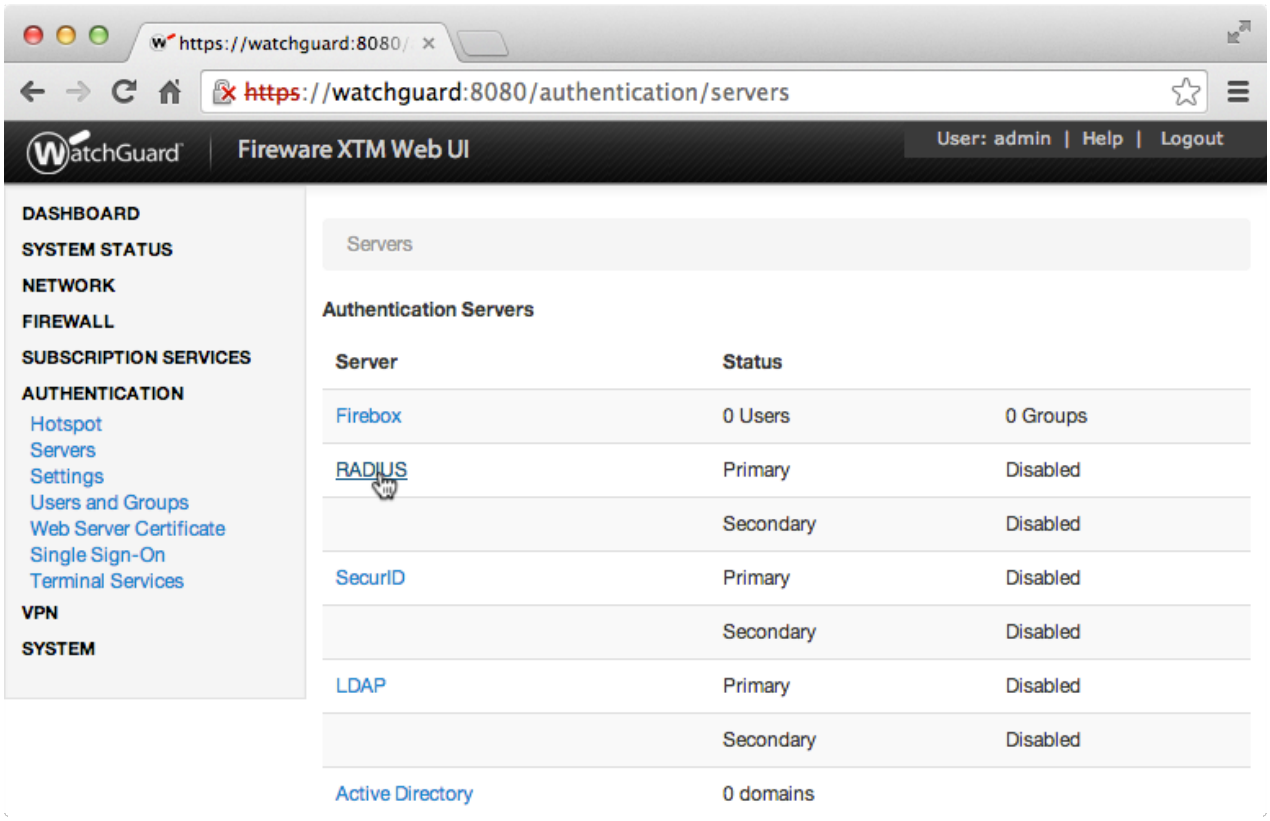
2. Click **Authentication**:



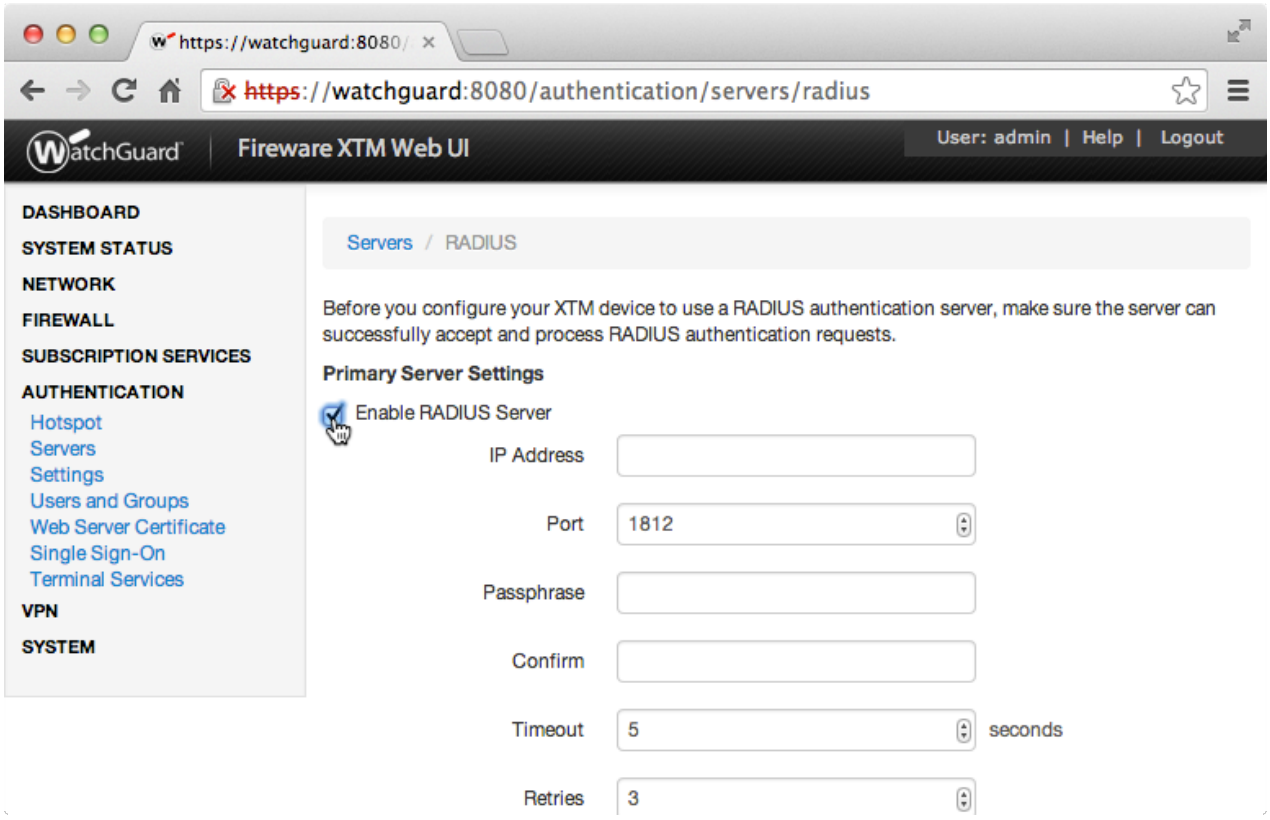
3. Under **Authentication** click **Servers**:



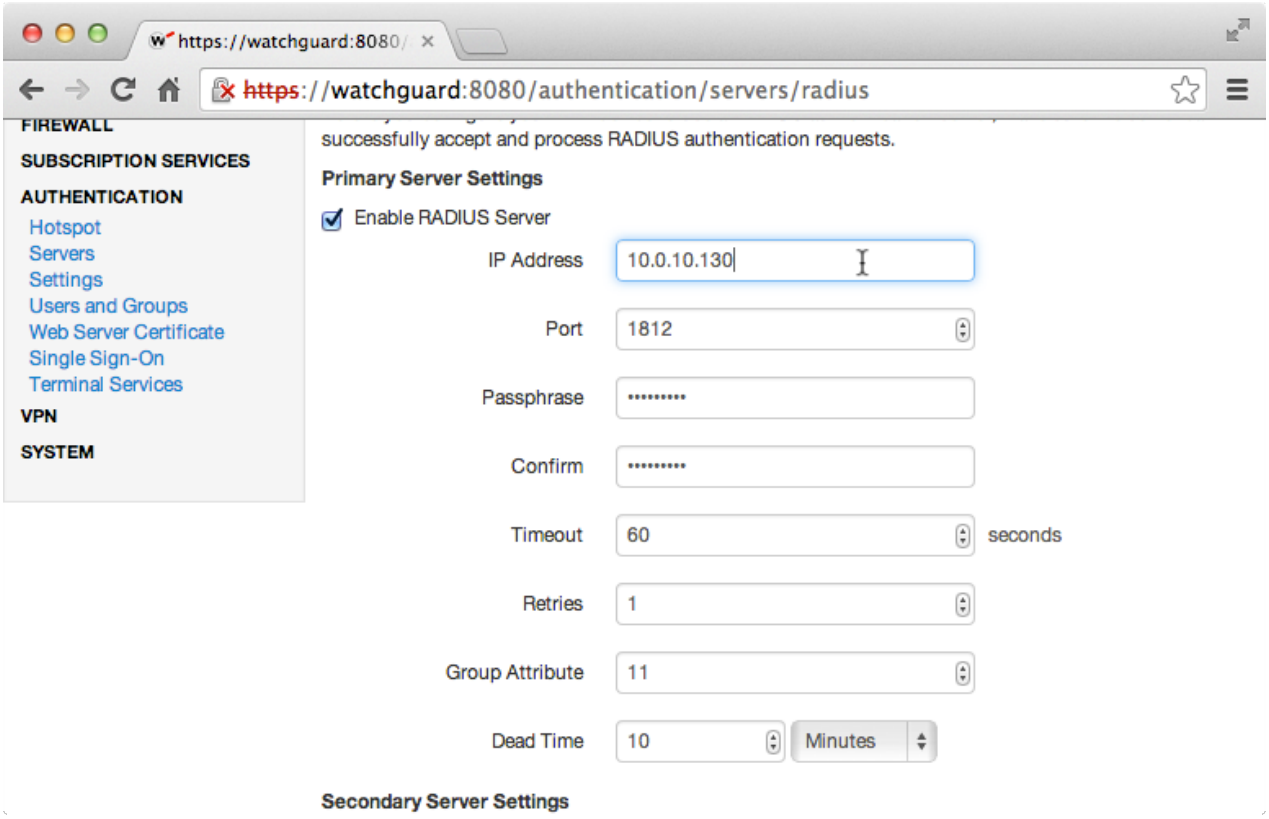
4. Under **Authentication Servers** click **RADIUS**:



5. Under **Primary Server Settings** click **Enable RADIUS Server**:



6. Complete **Primary Server Settings** form:



`IP Address`	Address of LoginTC RADIUS Connector	10.0.10.130
`Port`	RADIUS authentication port. Must be 1812.	1812
`Passphrase`	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret
`Confirm`	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret
`Timeout`	Amount of time in seconds to wait. At least 60s.	60
`Retries`	Amount of times to retry authentication. Must be 1.	1
`Group Attribute`	RADIUS Attribute to be populated with user group info. Must be 11.	11
`Dead Time`	Amount of time until session is considered dead.	10

Group Attribute and Access Control

WatchGuard devices can use the **Group Attribute** value to set the attribute that carries the User Group information. This information is used for access control. Configure `Group Attribute` in Active Directory / LDAP Option to include the Filter ID string with the user authentication message that gets sent to the Watchguard device.

For example set `RADIUS Group Attribute` to `Filter-Id` and `LDAP Group` to `engineerGroup` or `financeGroup`.

To test, navigate to your WatchGuard clientless VPN portal or use a WatchGuard client 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
   ```

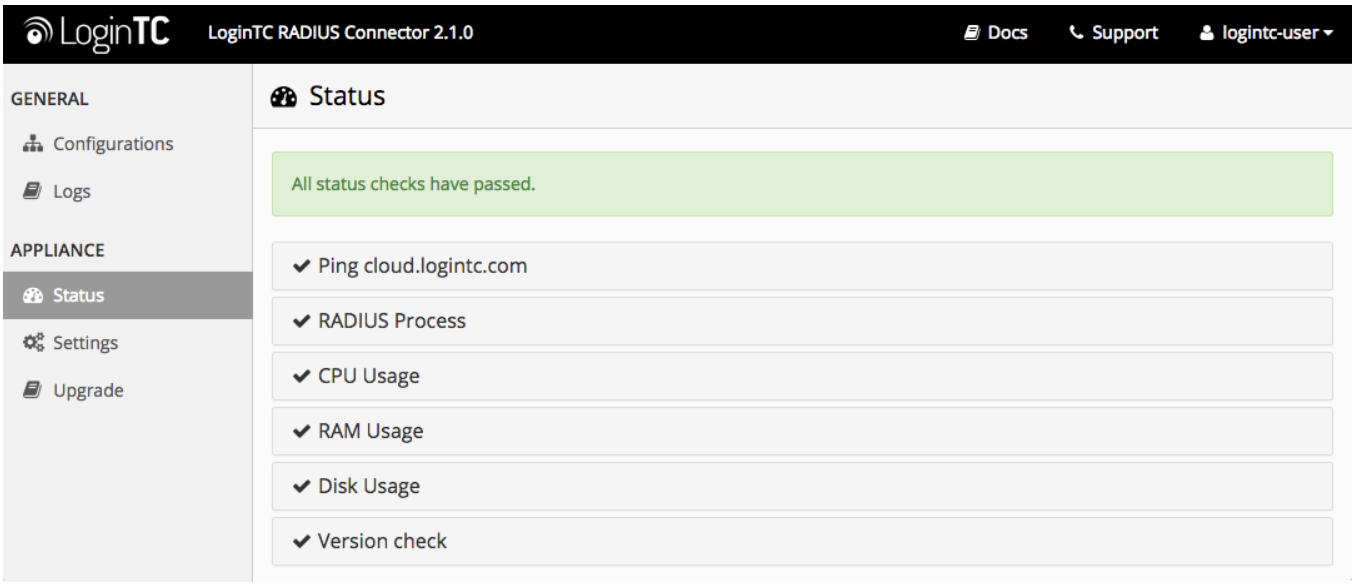
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

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

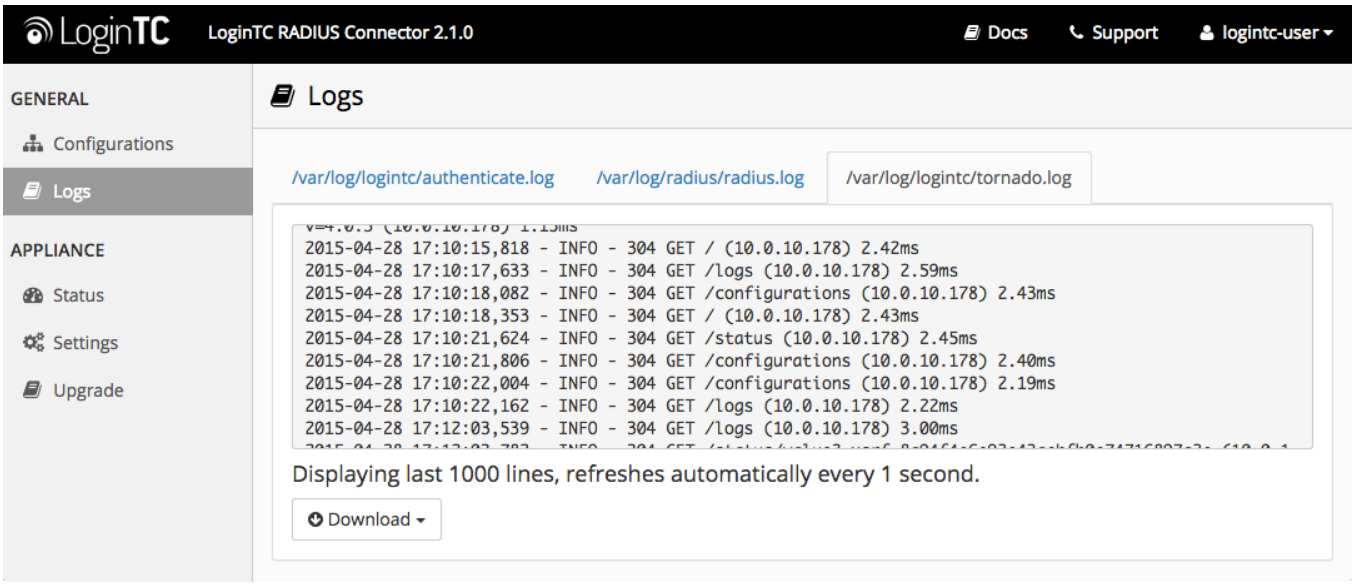
   Open the file and update the `DEVICE="eth0"` line to `DEVICE="eth1"`

Not Authenticating

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



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



Email Support

For any additional help please email 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 (2.1.1):

1. SSH into the virtual appliance or open the console (use same username / password as web GUI)
2. `cd /tmp`
3. `curl -O https://www.logintc.com/downloads/logintc-radius-connector-2.1.1-upgrade.tar.gz`
   (SHA-1: `8b3709611a8759911283cce9fce9efe4e628dfdb`)

4. `tar -xf logintc-radius-connector-2.1.1-upgrade.tar.gz`
5. `sudo sh logintc-radius-connector-2.1.1-upgrade/upgrade.sh`