Two factor authentication for WatchGuard XTM and Firebox IPSec Alternative

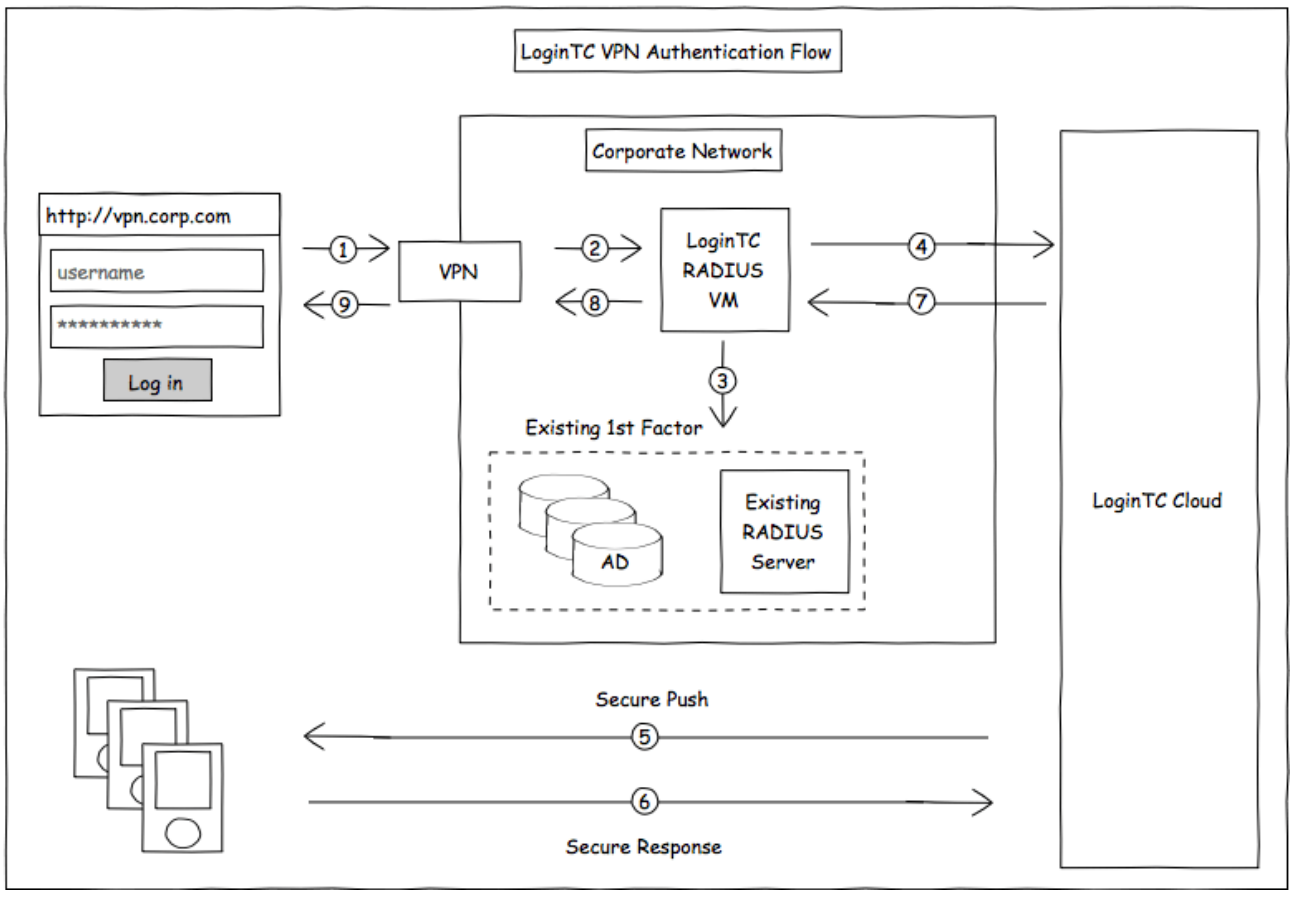
logintc.com/docs/connectors/watchguard-ipsec-alt.html

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables the WatchGuard XTM and Firebox VPN (e.g. **Mobile VPN with SSL or IPSec**) to use LoginTC for the most secure two-factor authentication. For an alternate method using Challenge Response then you may be interested in: Two factor authentication for WatchGuard Alternative.

User Experience

After entering the username and password into the Mobile VPN IPSec client, an authentication request is sent to the user's mobile device using a push notification. The user simply needs to approve the request for second factor.

Architecture / Compatibility



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

Appliance not listed?

We probably support it. Contact us if you have any questions.

Compatibility Guide

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

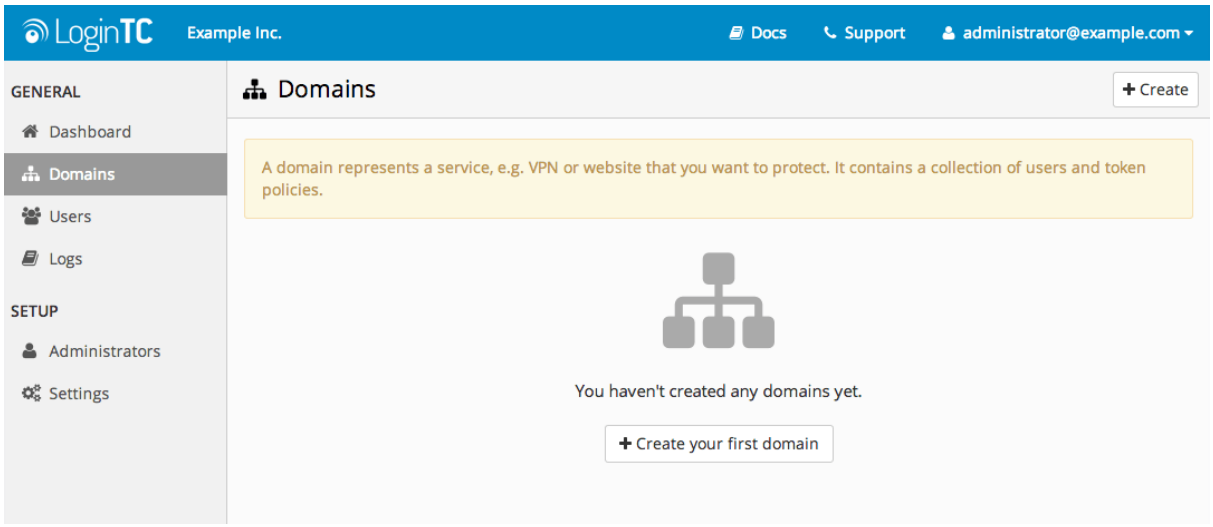
Prerequisites

Before proceeding, please ensure you have the following:

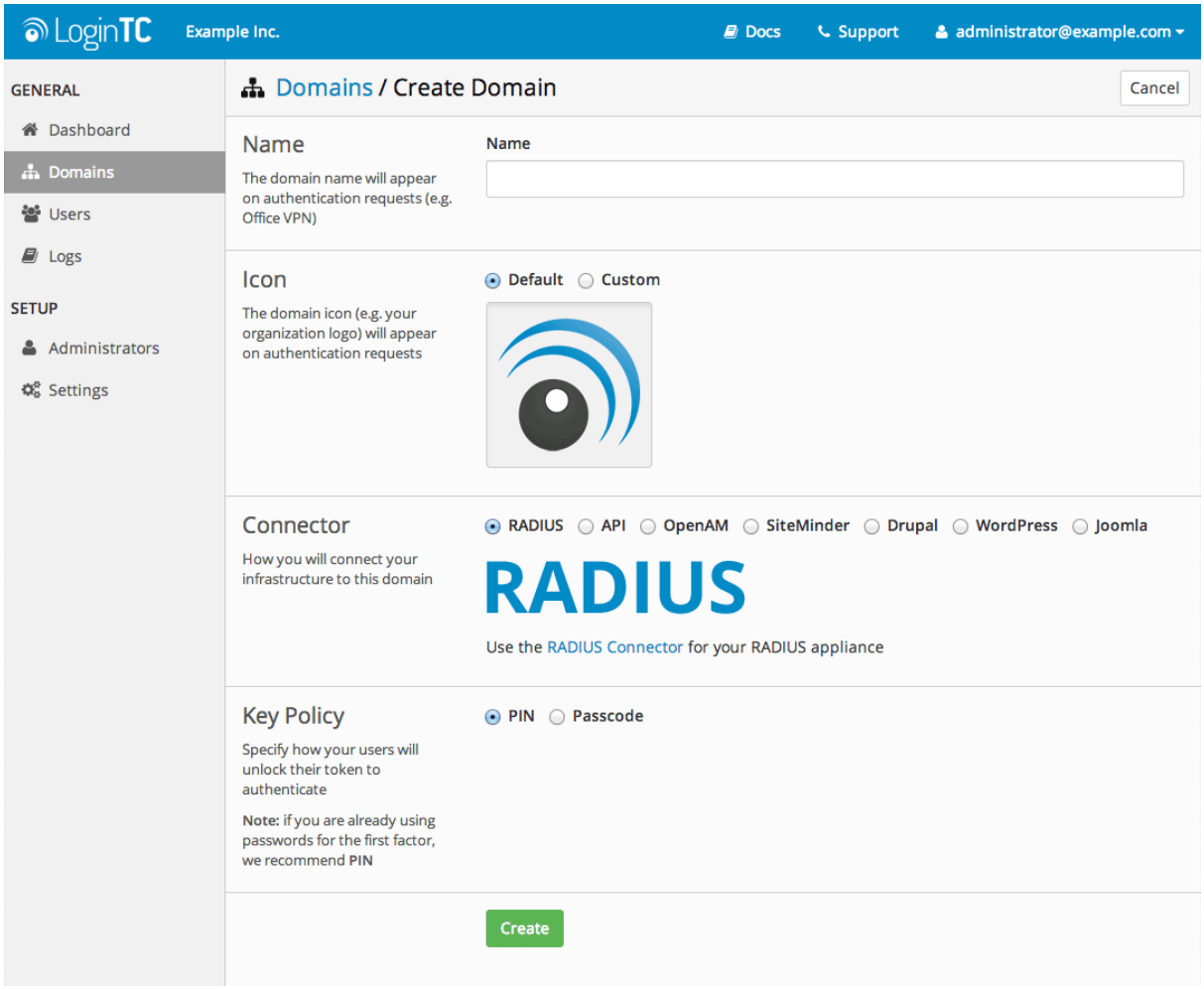
RADIUS Domain Creation

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 6.8 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)

Port	Protocol	Purpose
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

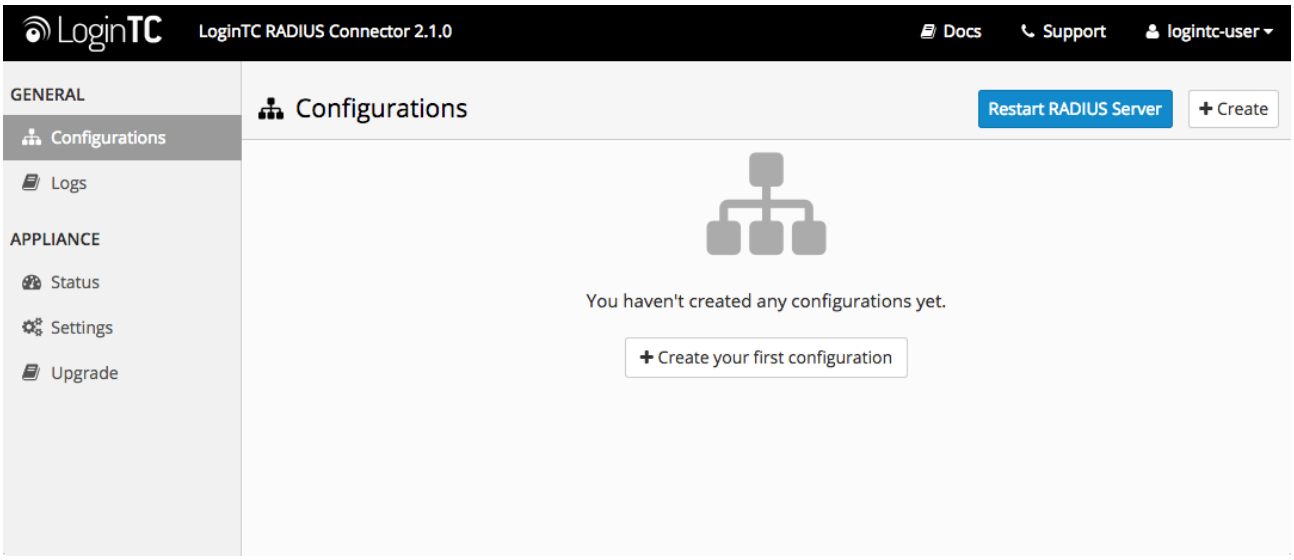
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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

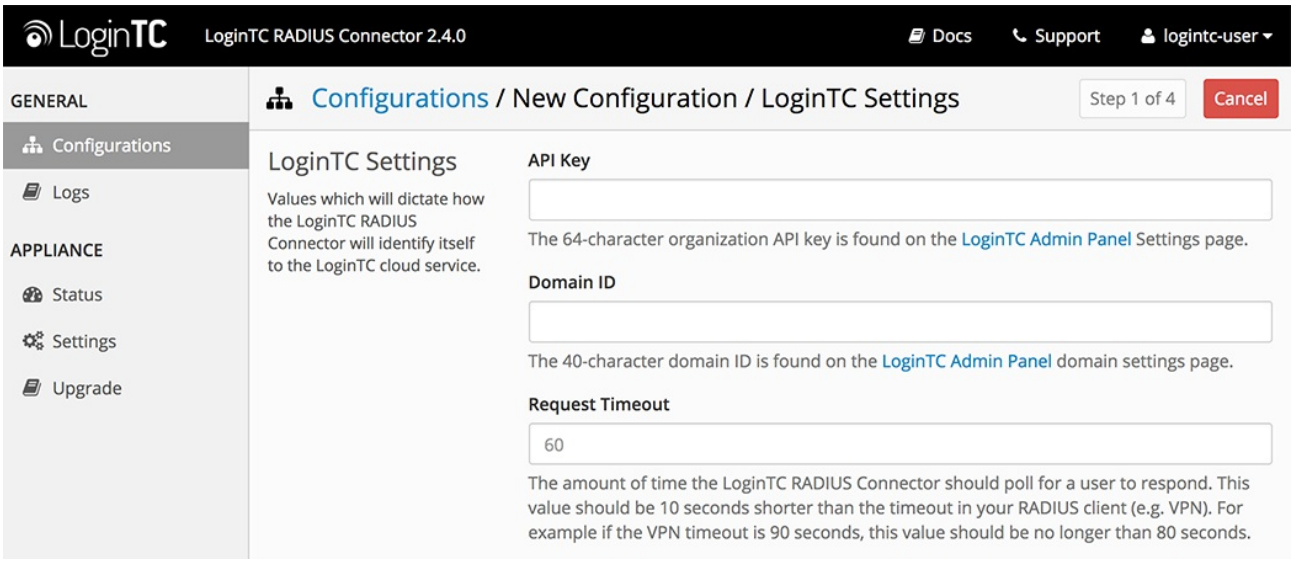
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



LoginTC Settings

Configure which LoginTC organization and domain to use:



Configuration values:

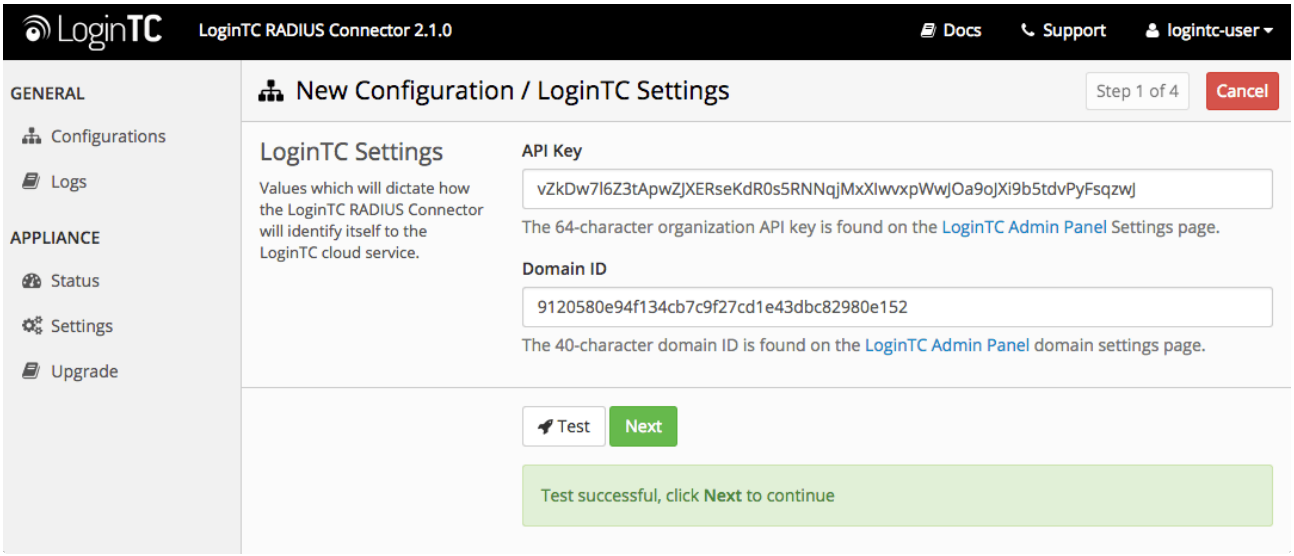
Property	Explanation
`API Key`	The 64-character organization API key
`Domain ID`	The 40-character domain ID
`Request Timeout`	Number of seconds that the RADIUS connector will wait for

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

Request Timeout

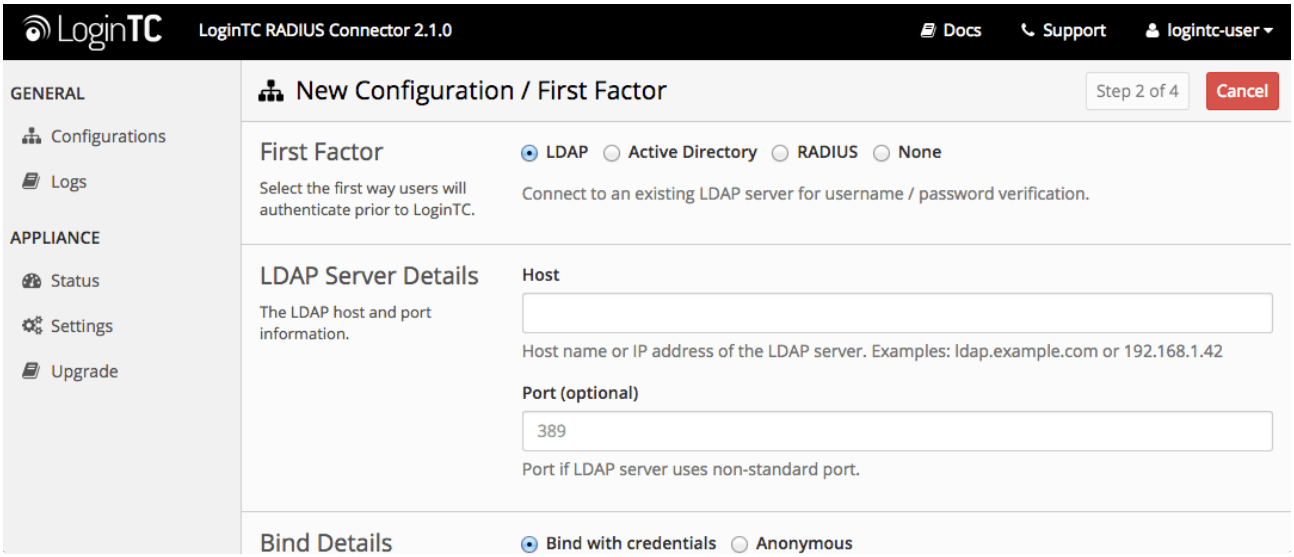
Make a note of what you set the Request Timeout to as you will need to use a larger timeout value in your WatchGuard. We recommend setting the Request Timeout value to 60 seconds in the LoginTC RADIUS Connector and setting the RADIUS authentication server timeout to 70 seconds in WatchGuard.

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



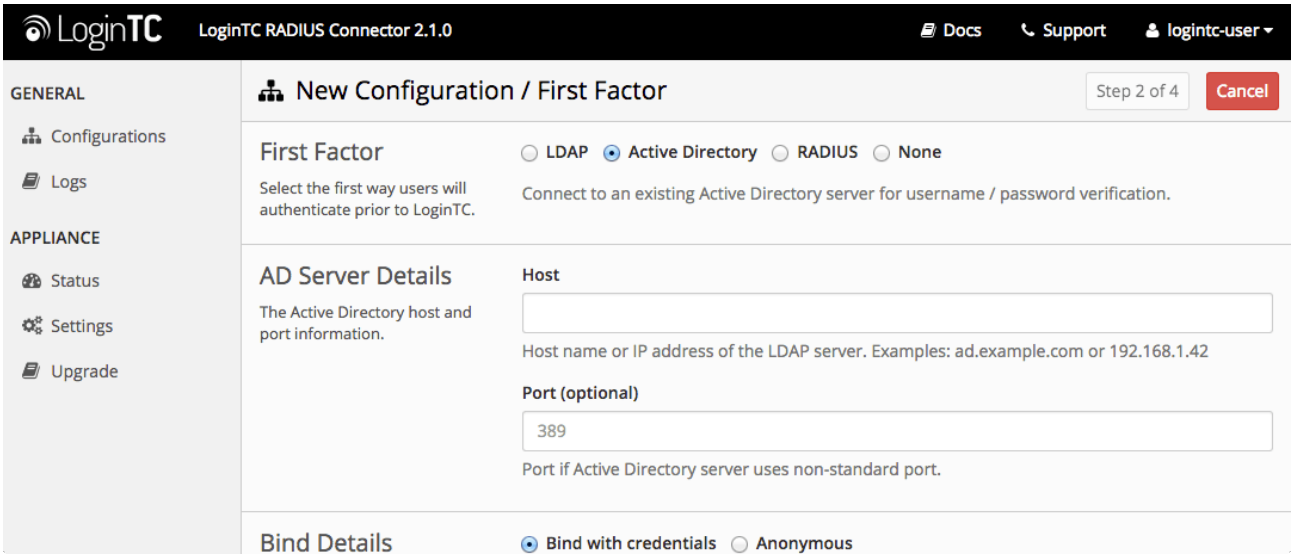
First Authentication Factor

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:

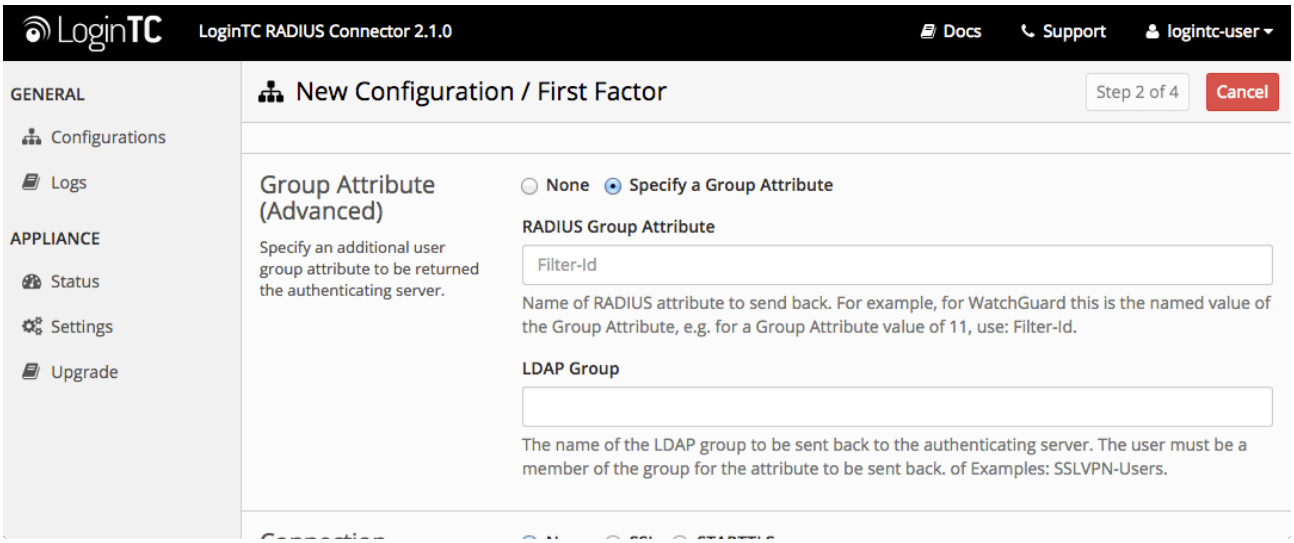
Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The 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.	`Office VPN`
`RADIUS Group Attribute` (optional)	Name of RADIUS attribute to send back	`Filter-Id`
`LDAP Group / AD Group` (optional)	A comma delimited list of the names of possible LDAP groups to be sent back to the authenticating server. The user must be a member of a group for the attribute to be sent back. Groups membership is checked in priority order, if the user is a member of multiple groups the first group matched is returned.	`Office VPN` or `Administrators,Sales,Engineers`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

Group Attribute and Access Control

In order to use Mobile VPN with IPSec, you must properly configure the **Group Attribute** in your RADIUS Connector. WatchGuard devices use the Group Attribute value to set the attribute that carries the User Group information. This information is used for access control.

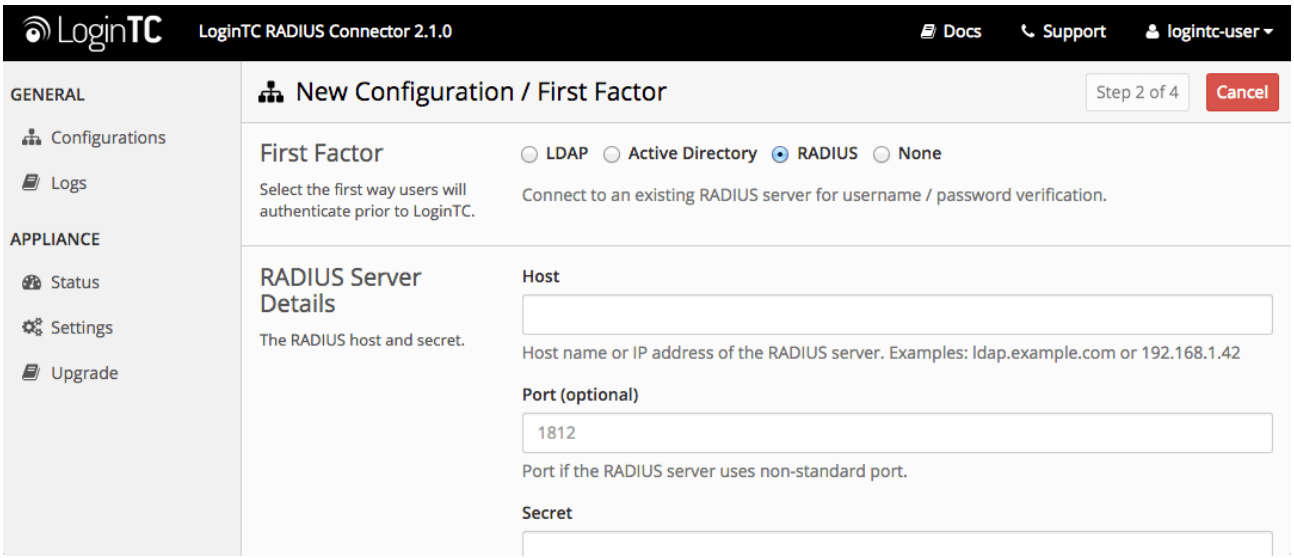
LDAP Group / AD Group : The name of a group in the LDAP Directory that all authenticating users belong to. The group name must match exactly the Mobile VPN with IPSec group profile name.



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:

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

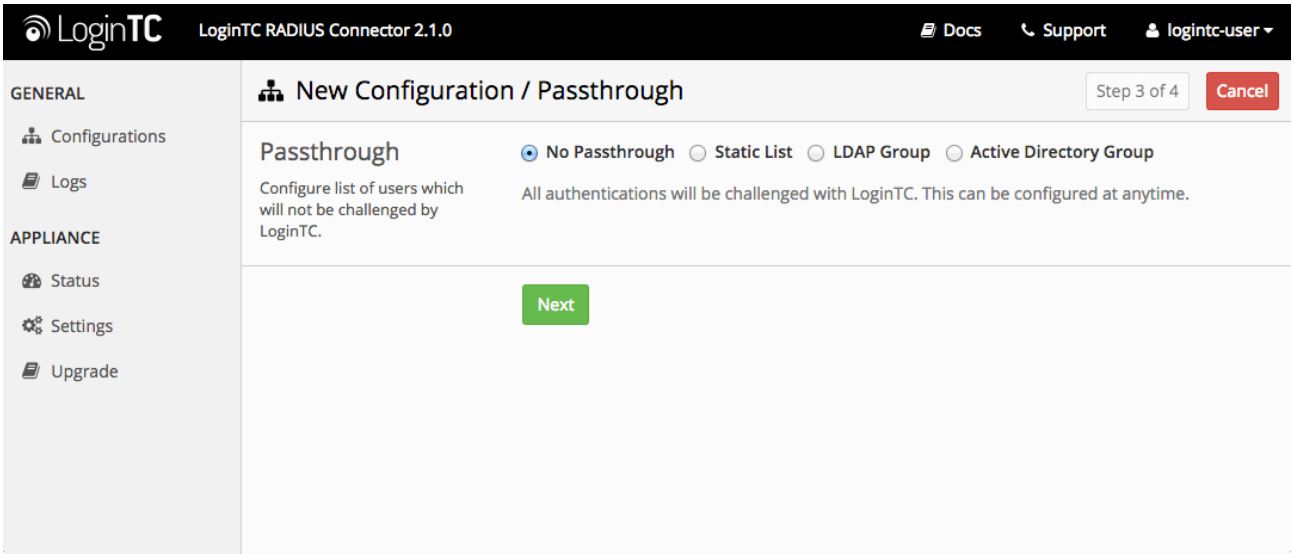
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.

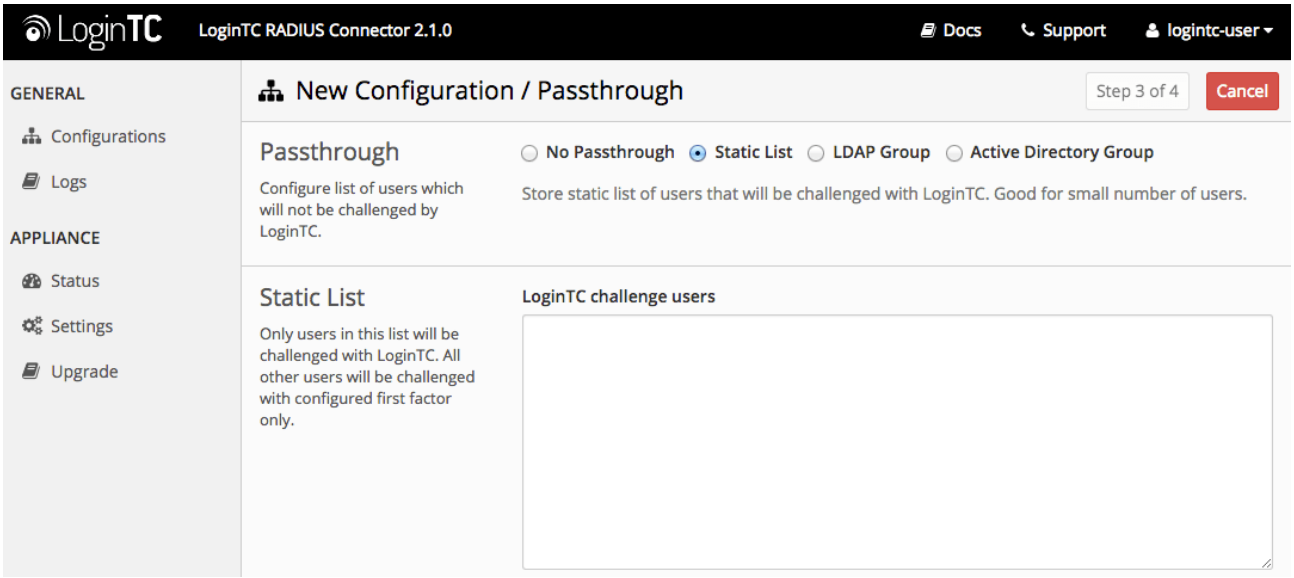
No Passthrough (default)

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



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.

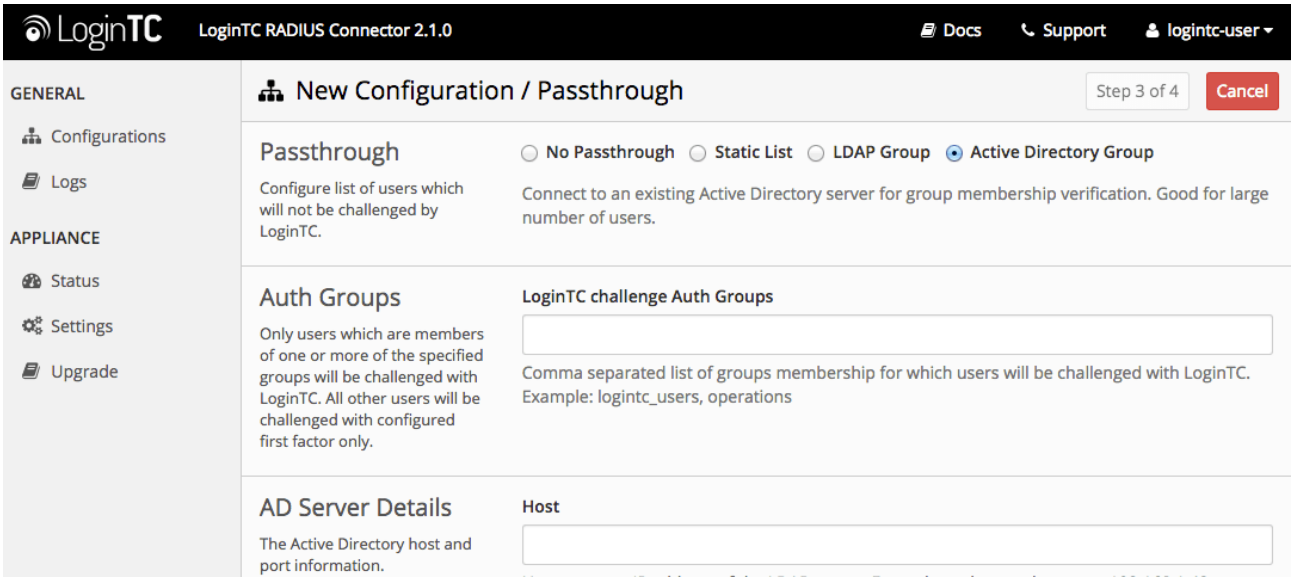


LoginTC challenge users: a new line separated list of usernames. For example:

```
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	`Office VPN` or `two-factor-users`
`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`

Property	Explanation	Examples
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

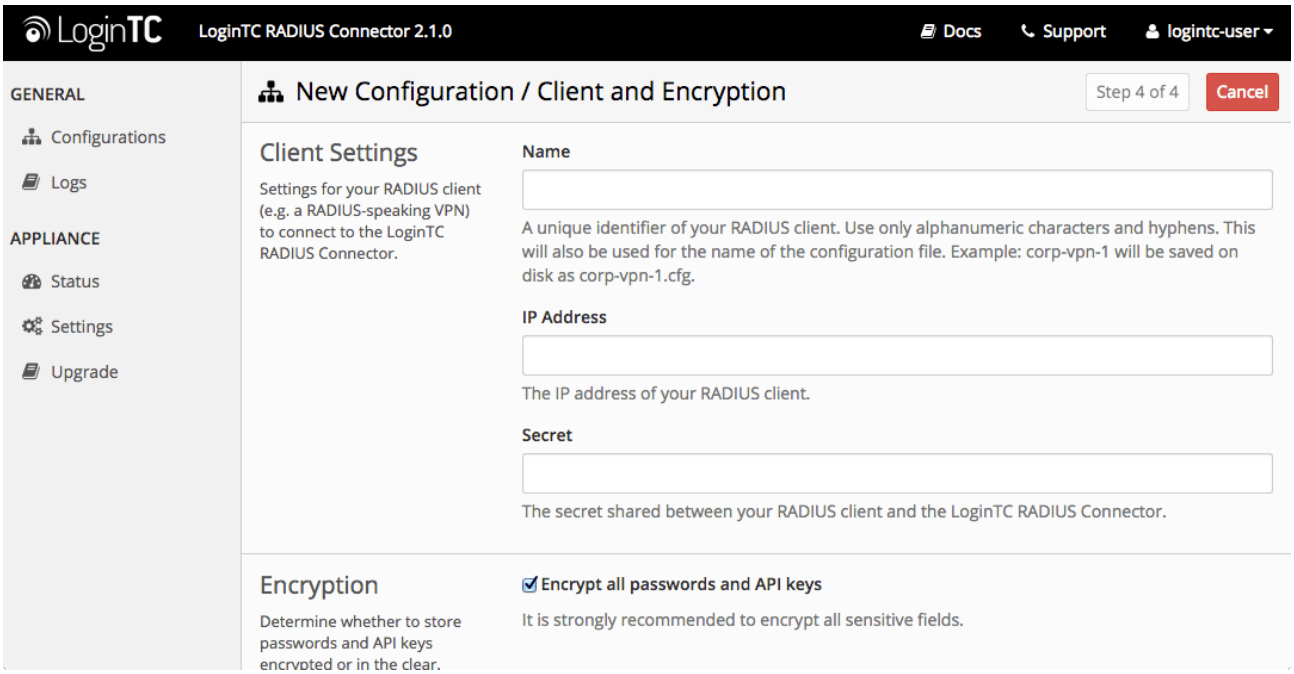
Configuration Simplified

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

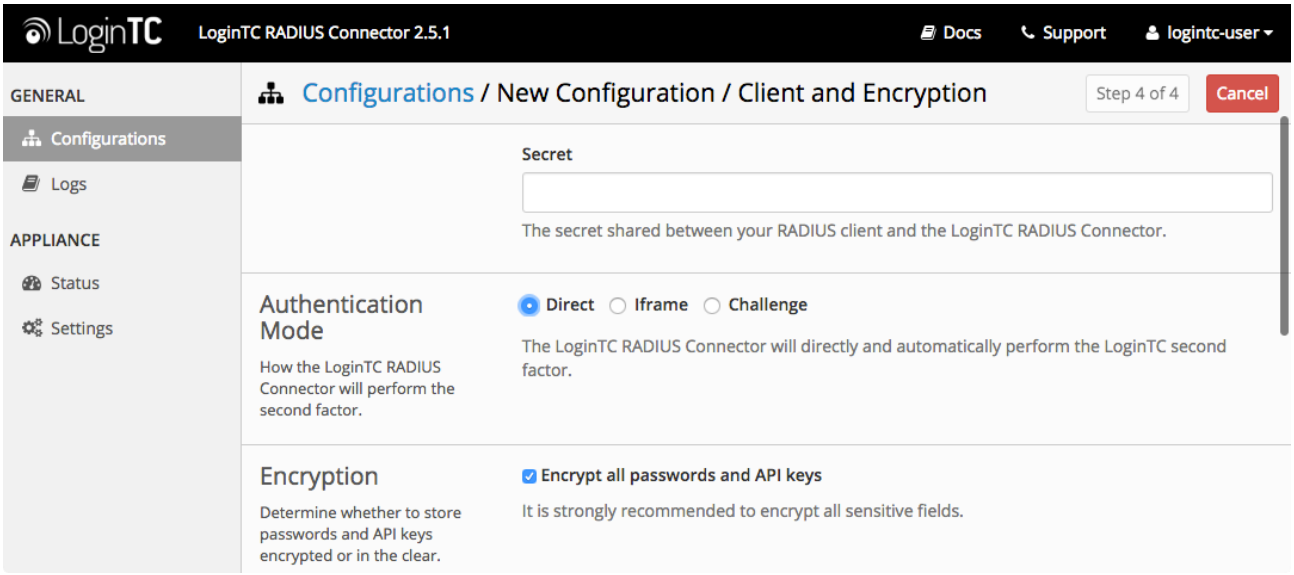
Configure RADIUS client (e.g. your RADIUS-speaking VPN):



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`

Under Authentication Mode select **Direct**

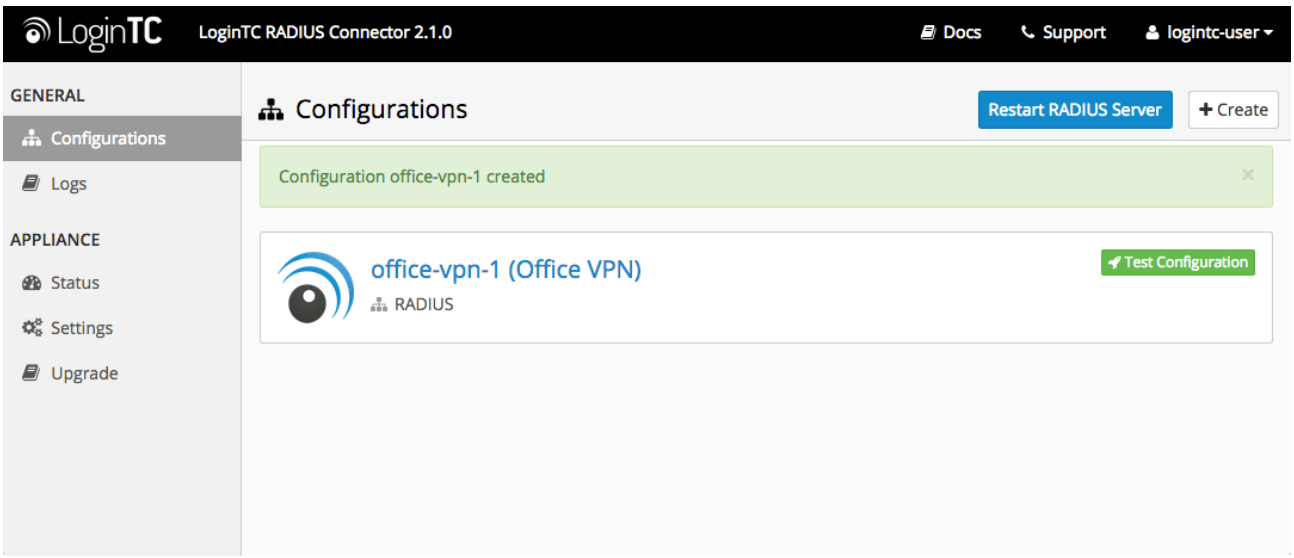


The LoginTC RADIUS Connector will directly and automatically perform the LoginTC second factor. See User Experience for more information.

Data Encryption

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

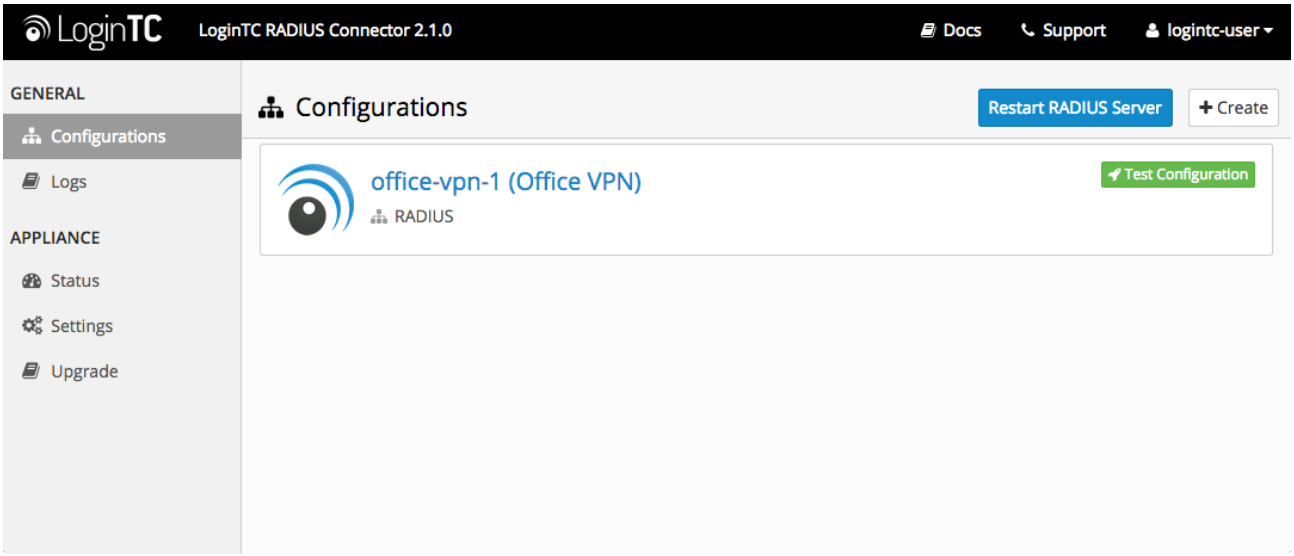
Click **Test** to validate the values and then click **Save**.



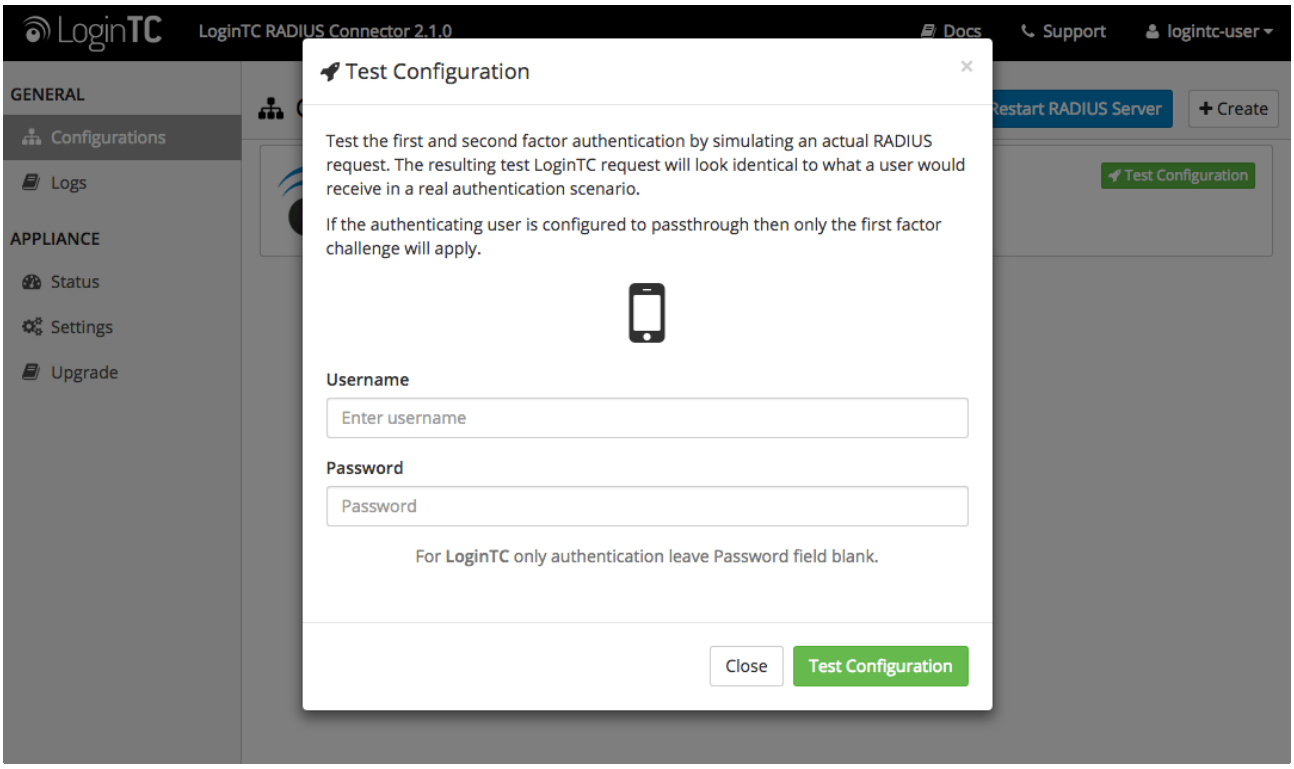
Testing (Connector)

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:

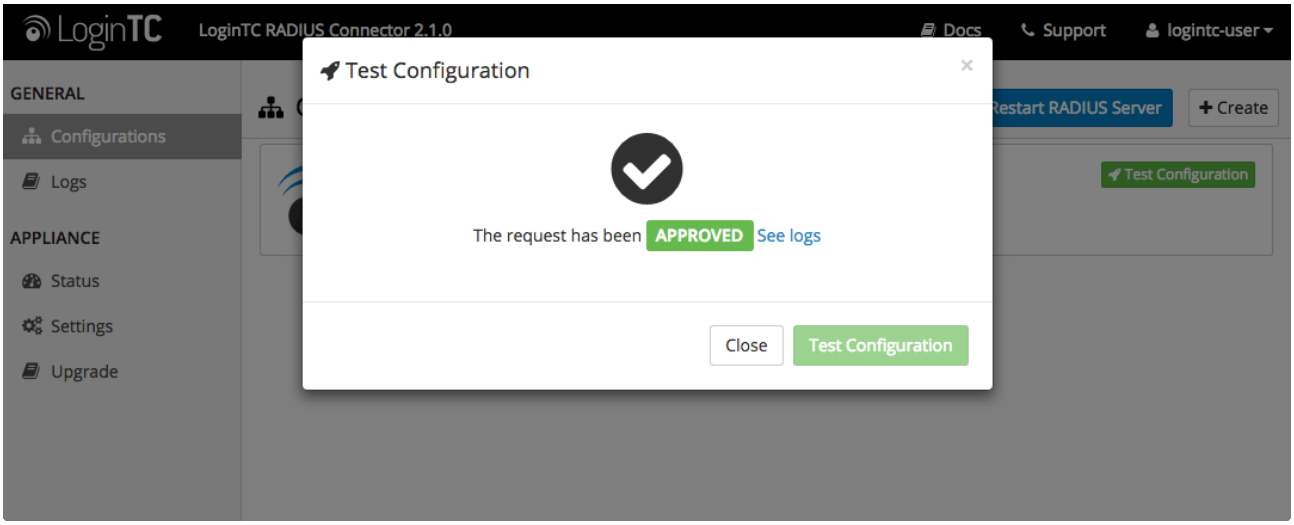
When you have loaded a token for your new user and domain, navigate to your appliance**web interface** URL:



Click **Test Configuration**:

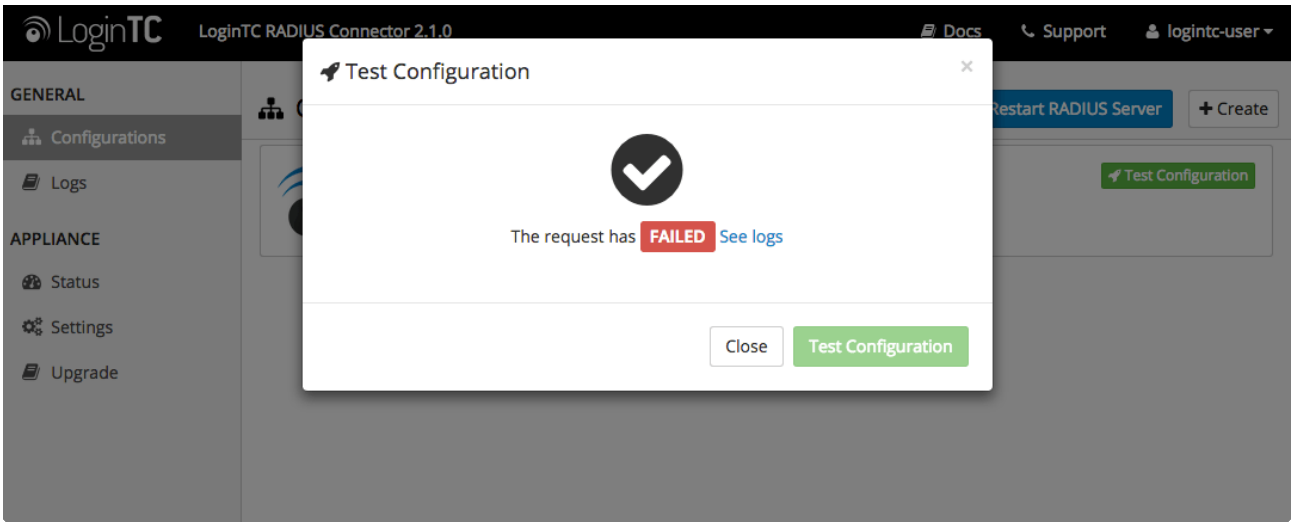


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

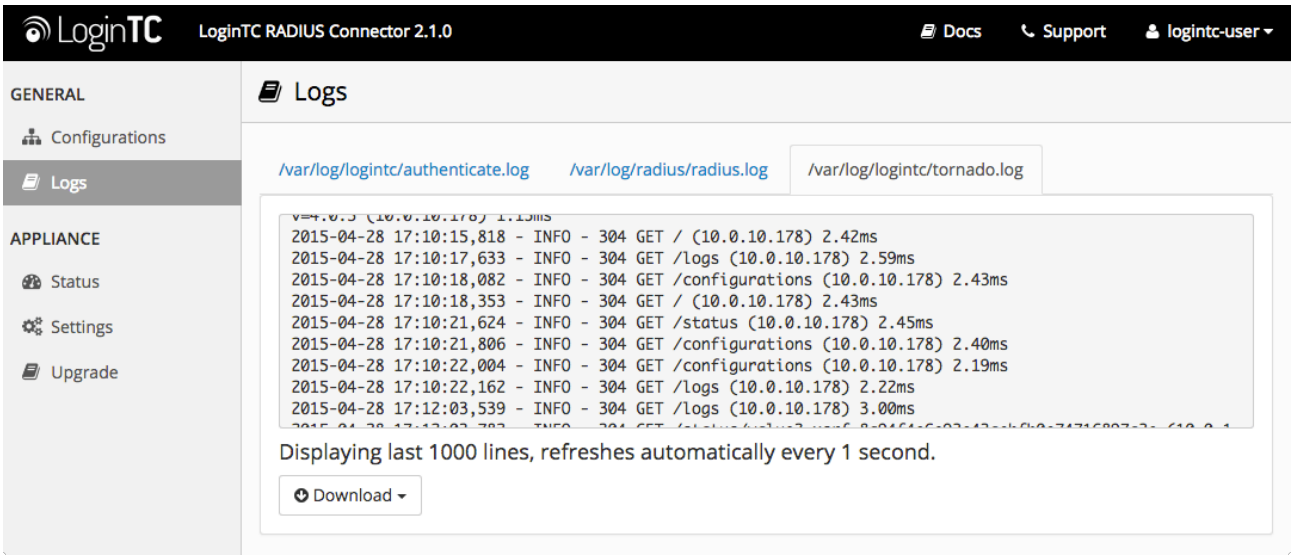


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



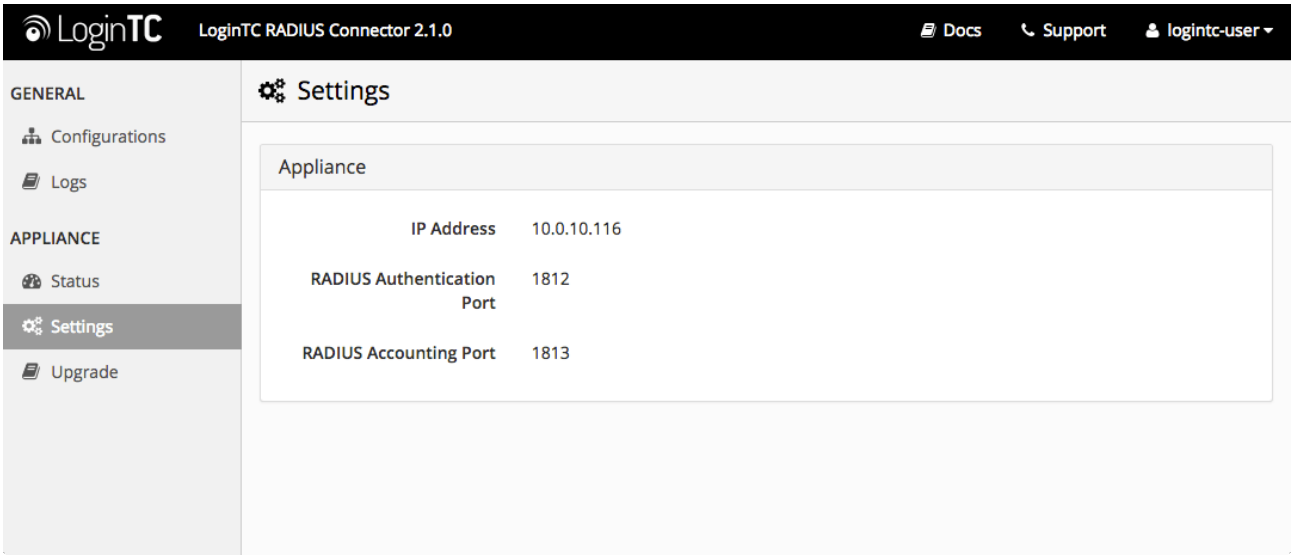
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:



WatchGuard - Quick Config Guide

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

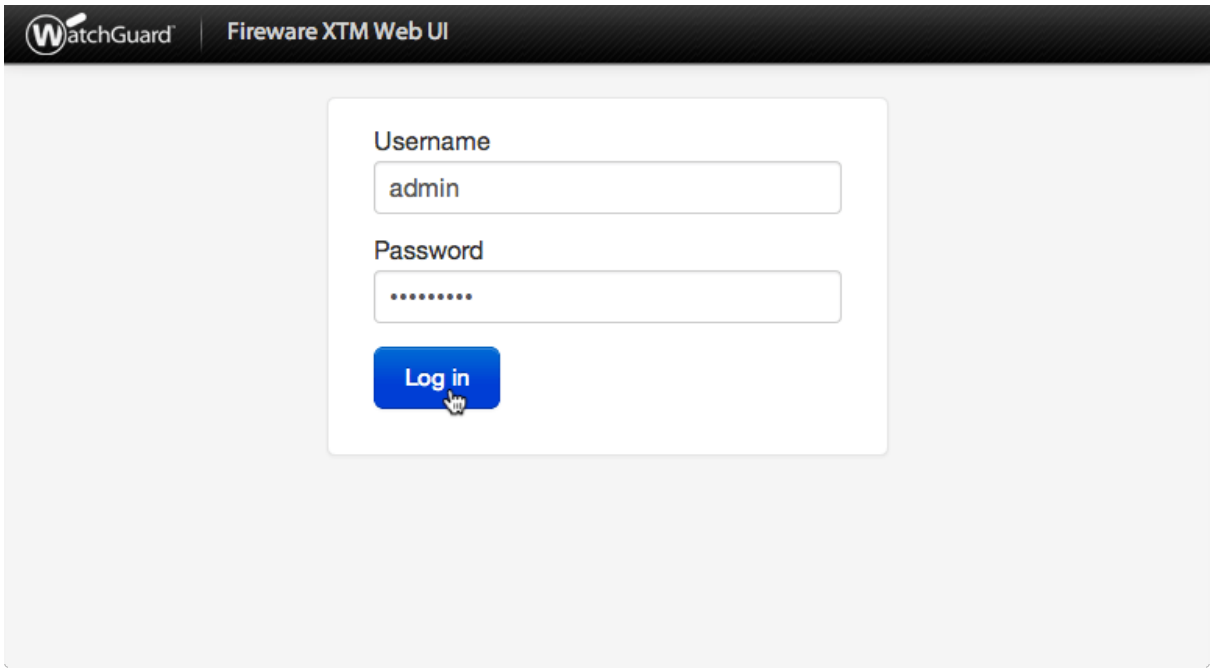
For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:



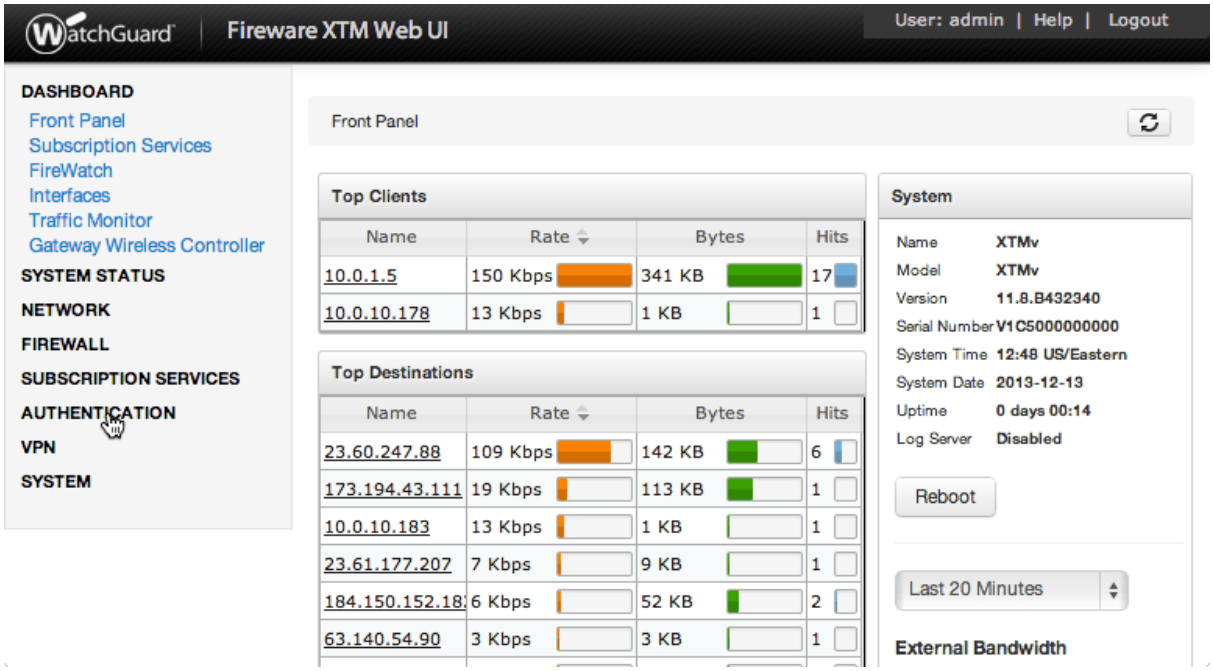
The following are quick steps to get VPN access protected with LoginTC. The instructions can be used for existing setups as well. Although these were performed on WatchGuard Fireware XTM Web UI, the same is true for other devices in the XTM series.

Mobile VPN with IPsec

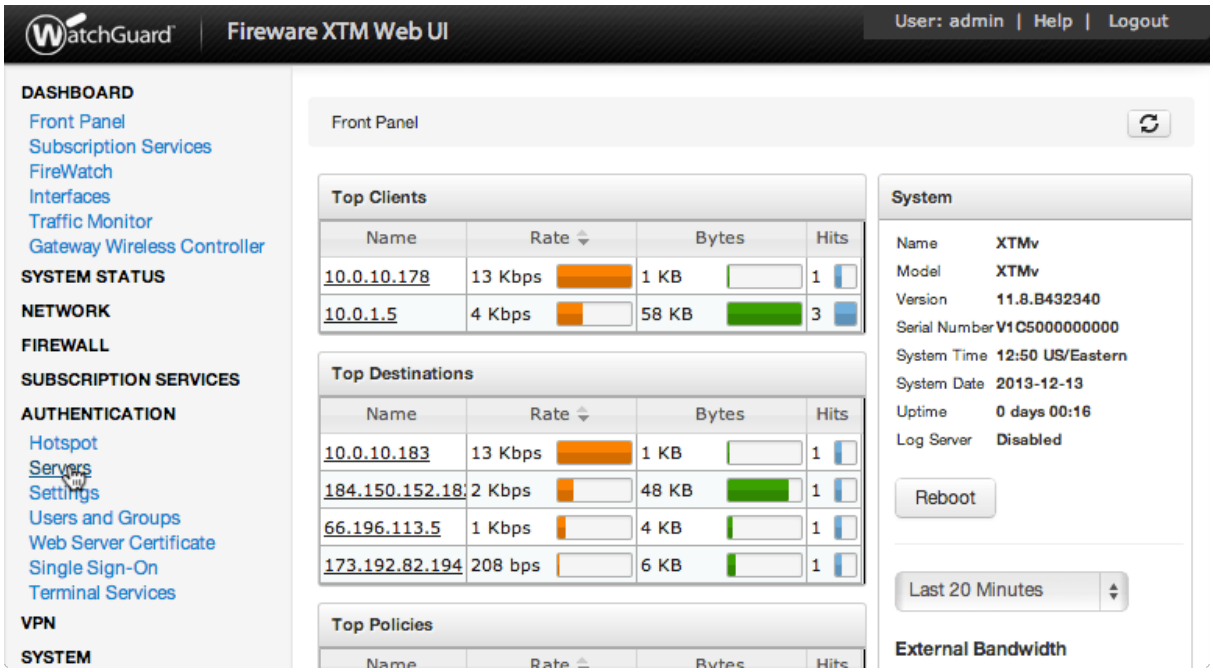
1. Log in to your WatchGuard (Fireware XTM Web UI)



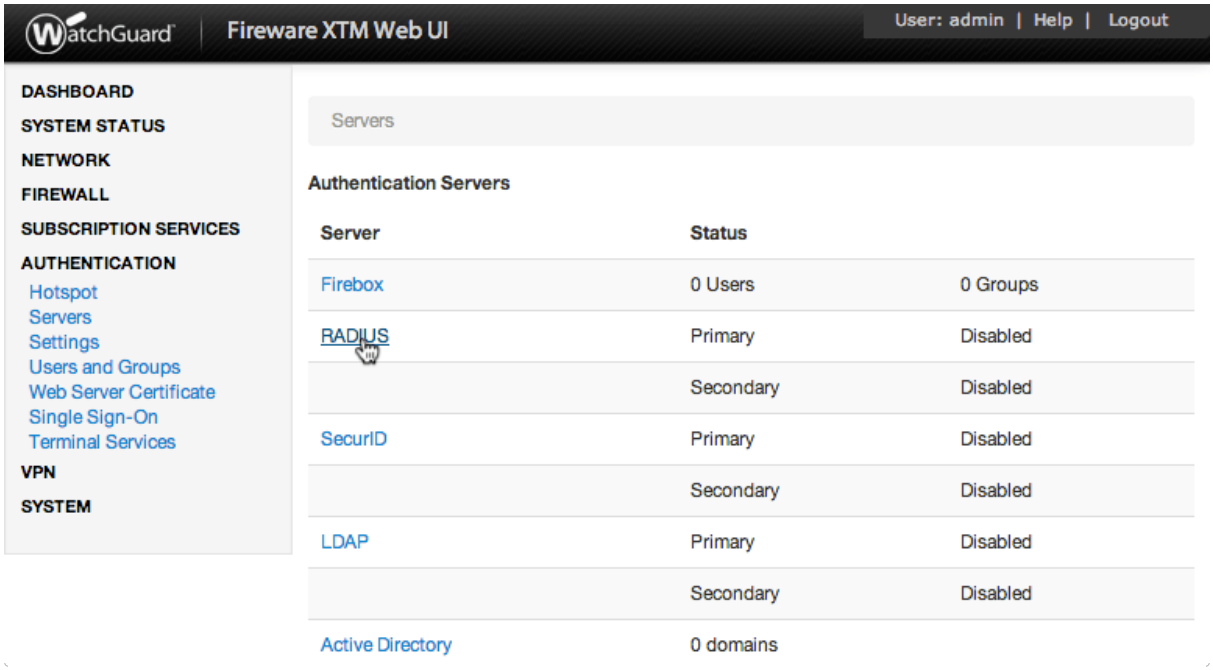
2. Click **Authentication**:



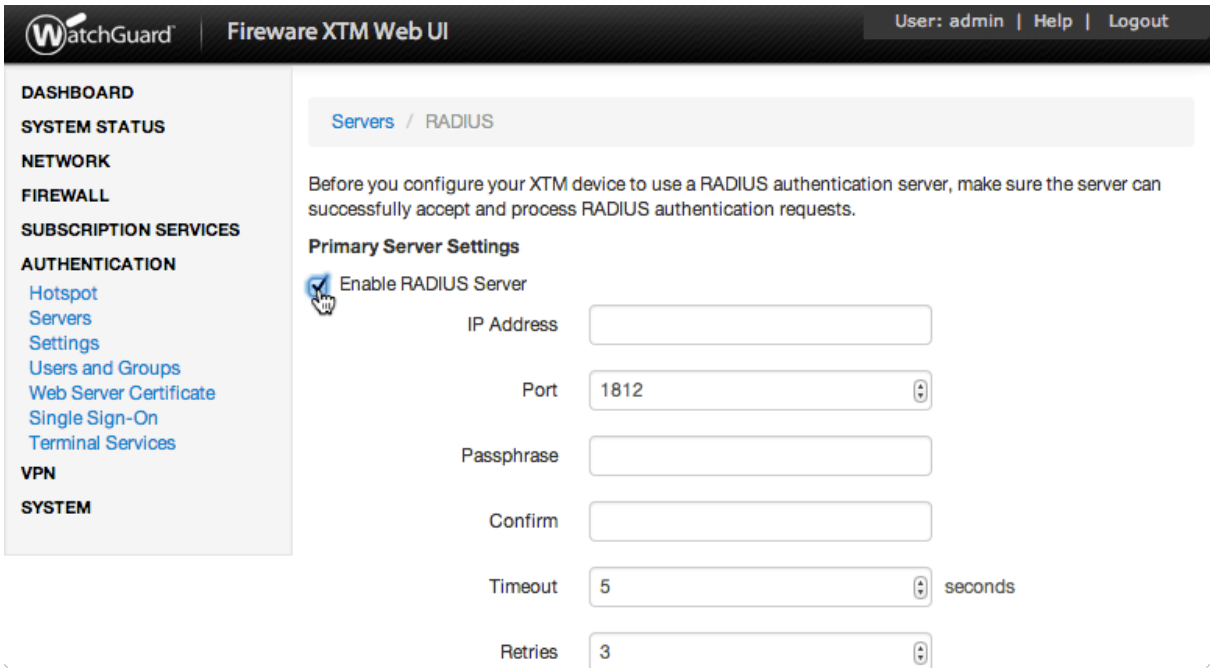
3. Under **Authentication** click **Servers**:



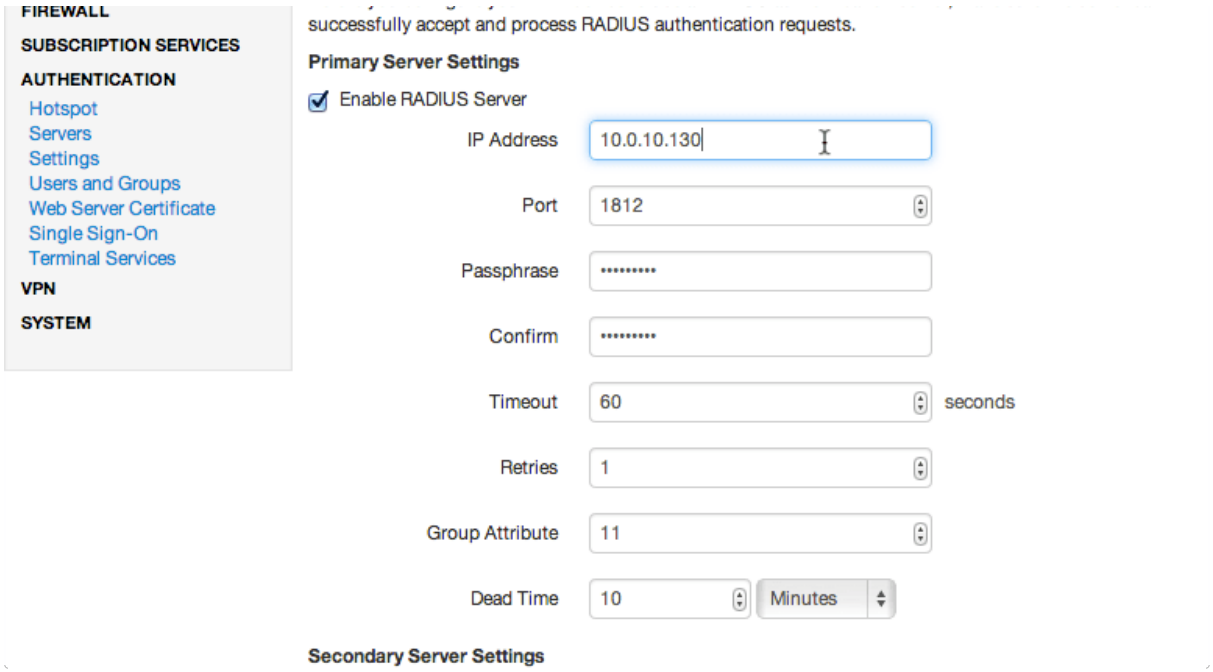
4. Under **Authentication Servers** click **RADIUS**:



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



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

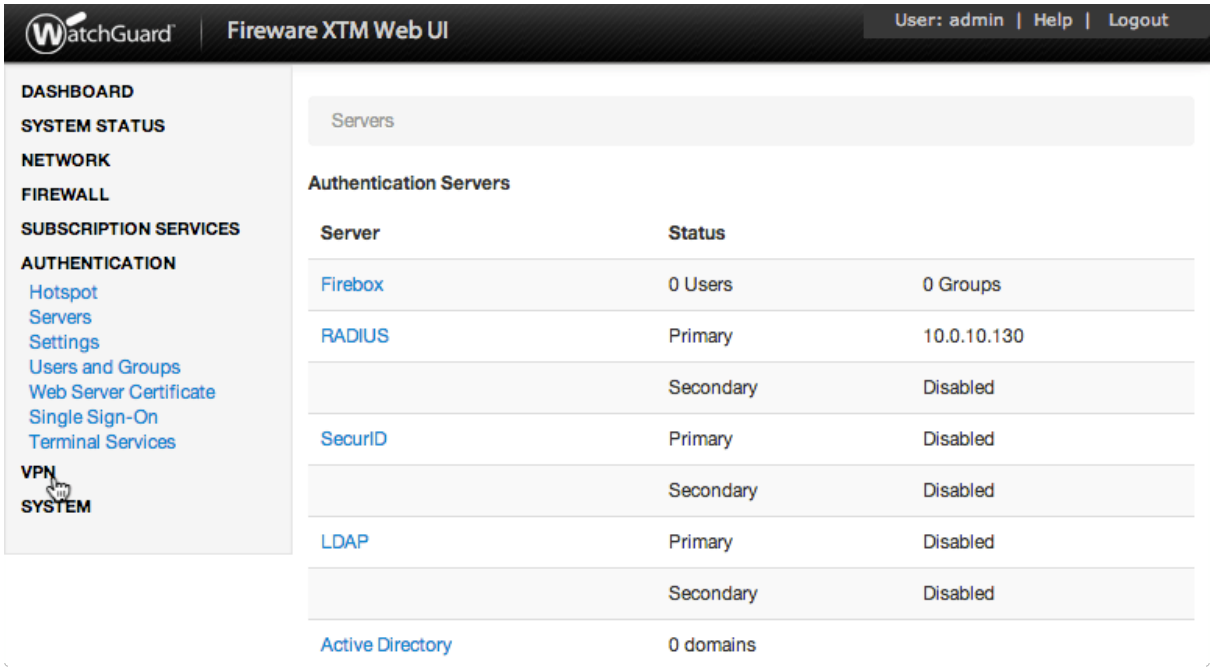


Property	Explanation	Example
`IP Address`	Address of LoginTC RADIUS Connector	10.0.10.130
`Port`	RADIUS authentication port. Must be 1812.	1812
`Passphrase`	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret
`Confirm`	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret
`Timeout`	Amount of time in seconds to wait. At least 90s.	90
`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 when using SSL.	11
`Dead Time`	Amount of time an unresponsive RADIUS server is marked as inactive	10

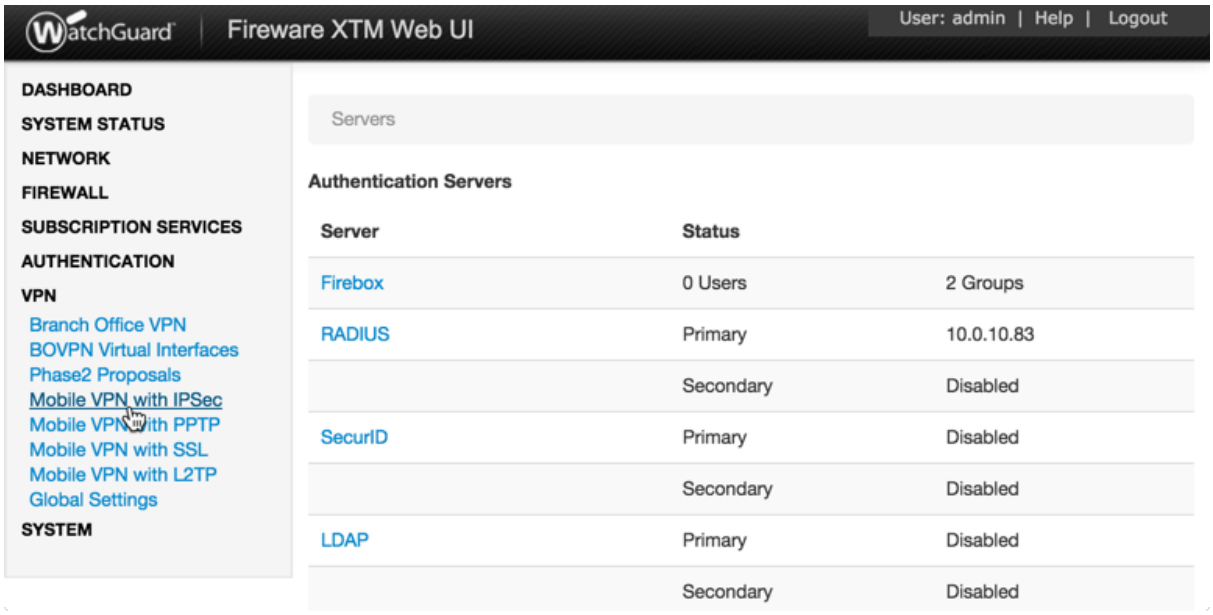
Group Attribute and Access Control

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 by certain VPN protocols.

7. Click **VPN**:

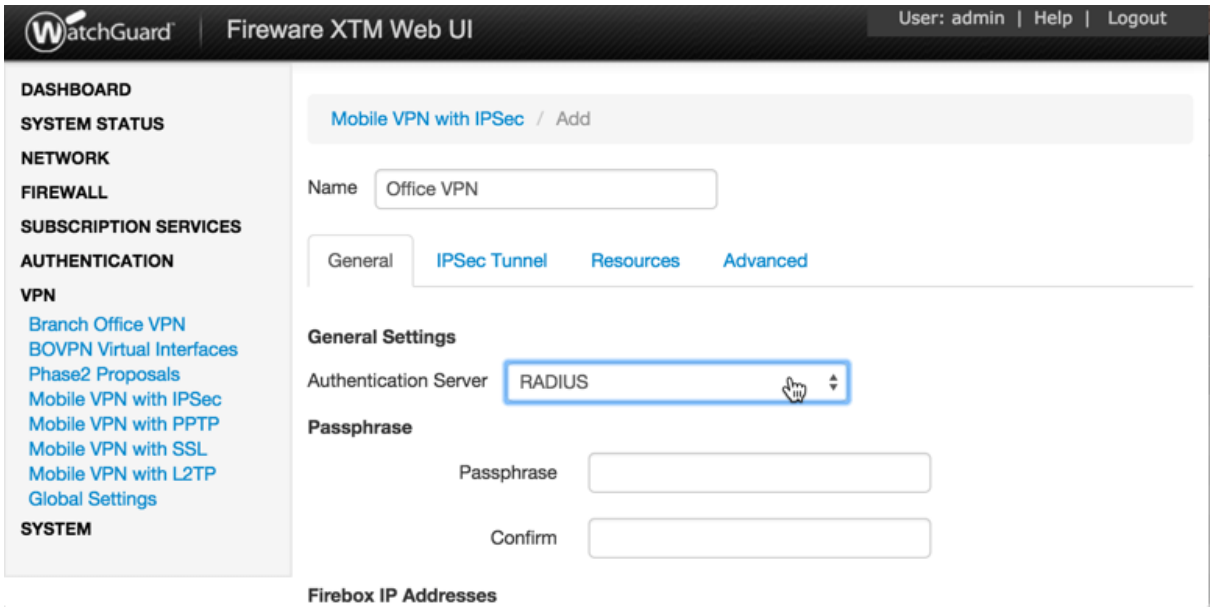


8. Under **VPN** click **Mobile VPN with IPsec**



9. Click **Add** to create a new group. Note that the name of the group does not have to match any of the groups names in the LDAP Directory

10. In **General Settings**, complete the form and select **RADIUS** as the authentication server.



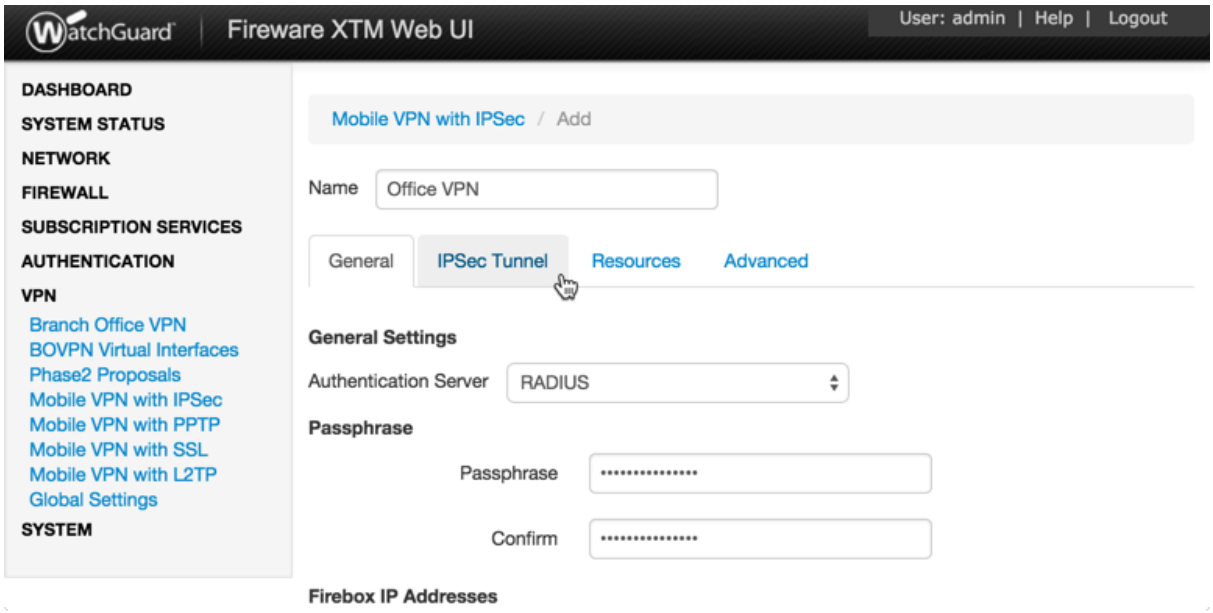
Property	Explanation	Example
`Name`	A unique name for this group configuration. This name must match exactly the LDAP / AD group name configured in First Factor authentication Group Attribute (advanced).	Office VPN
`Authentication Server`	The type of device that users of this group will be authenticated with.	Radius
`Passphrase`	The secret shared between the Mobile VPN client and the RADIUS server. The secret must be provided to all IPsec users.	sharedsecret
`Confirm`	The secret shared between the Mobile VPN client and the RADIUS server.	sharedsecret
`Primary`	Primary IP address or domain name Firebox users connect to.	10.0.10.130

Property	Explanation	Example
`Backup` (optional)	Secondary IP address or domain name Firebox users connect to.	10.0.10.131

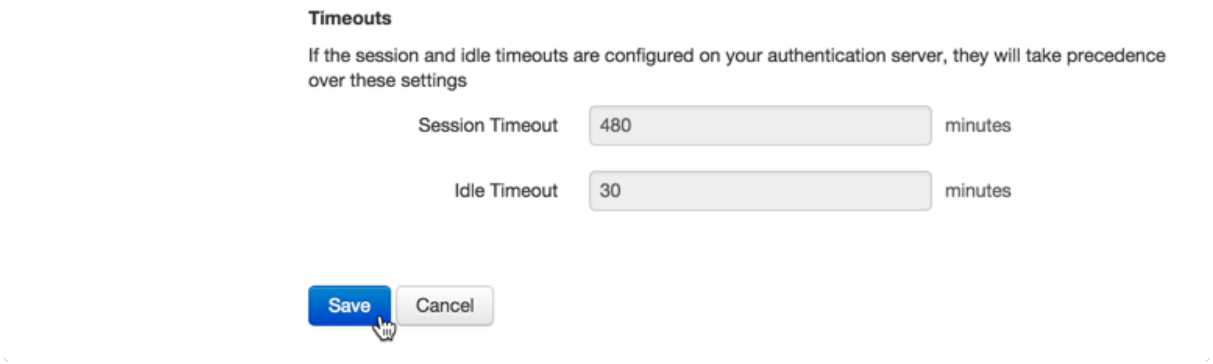
Mobile VPN with IPSec group profile name

In order to use Mobile VPN with IPSec, the Mobile VPN with IPSec group profile name must match exactly the LDAP / AD group name configured in First Factor authentication Group Attribute (advanced).

11. Fill out the forms under the **IPsec Tunnel**, **Resources**, and **Advanced** tabs to match the settings of your client. For more information about IPsec client configurations, check the WatchGuard Documentation



12. Click **Save**



You are now ready to test your configuration.

To test IPsec connections, use an IPsec VPN client such as the WatchGuard Mobile Application.

User Management

There are several options for managing your users within LoginTC:

Failover

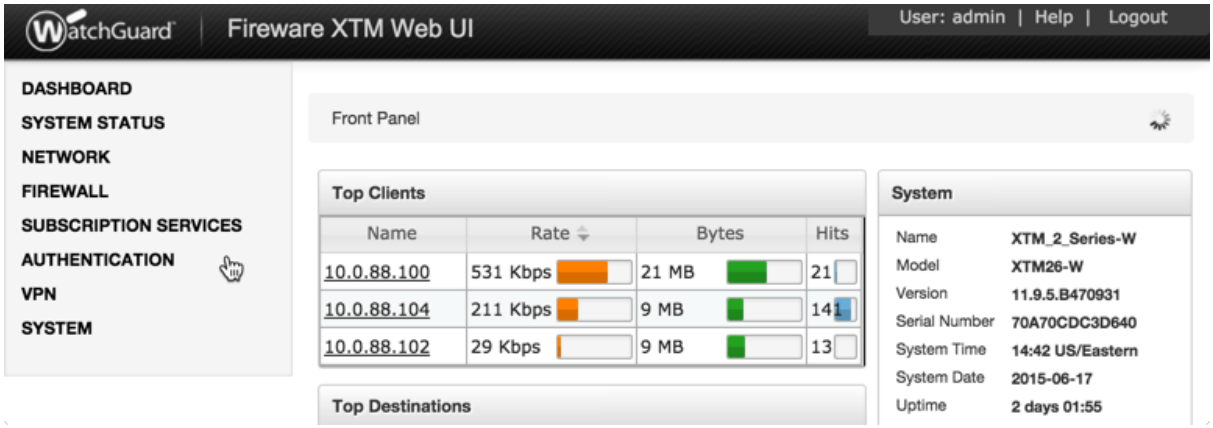
WatchGuard devices have built-in settings that make it easy to configure a secondary RADIUS server to provide failover.

> After three authentication attempts fail, Fireware XTM uses the secondary RADIUS server for the next authentication attempt. If the secondary server also fails to respond after three authentication attempts, Fireware XTM waits for the **Dead Time** interval (10 minutes by default) to elapse. After the Dead Time interval has elapsed, Fireware XTM tries to use the primary RADIUS server again.

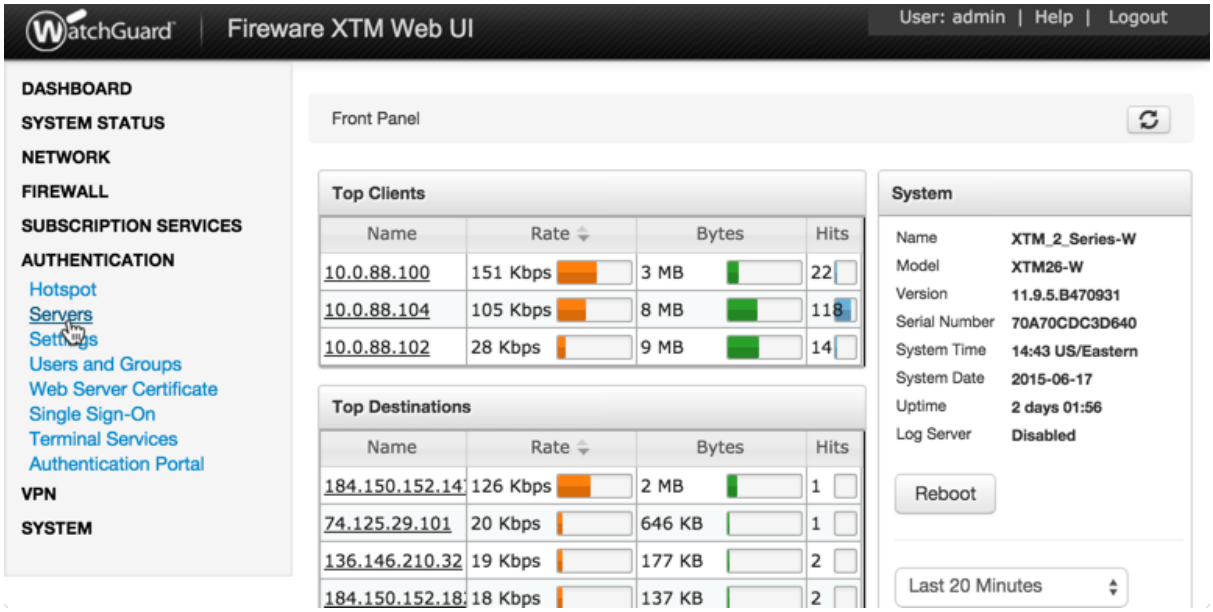
— *WatchGuard System Manager Help*

To set up another RADIUS server, deploy the downloaded LoginTC Connector again (you can deploy it multiple times) and configure it using the same settings as the first one. Click here to review the Connector configuration process. Afterwards, login to your **WatchGuard Web UI** and make the following changes:

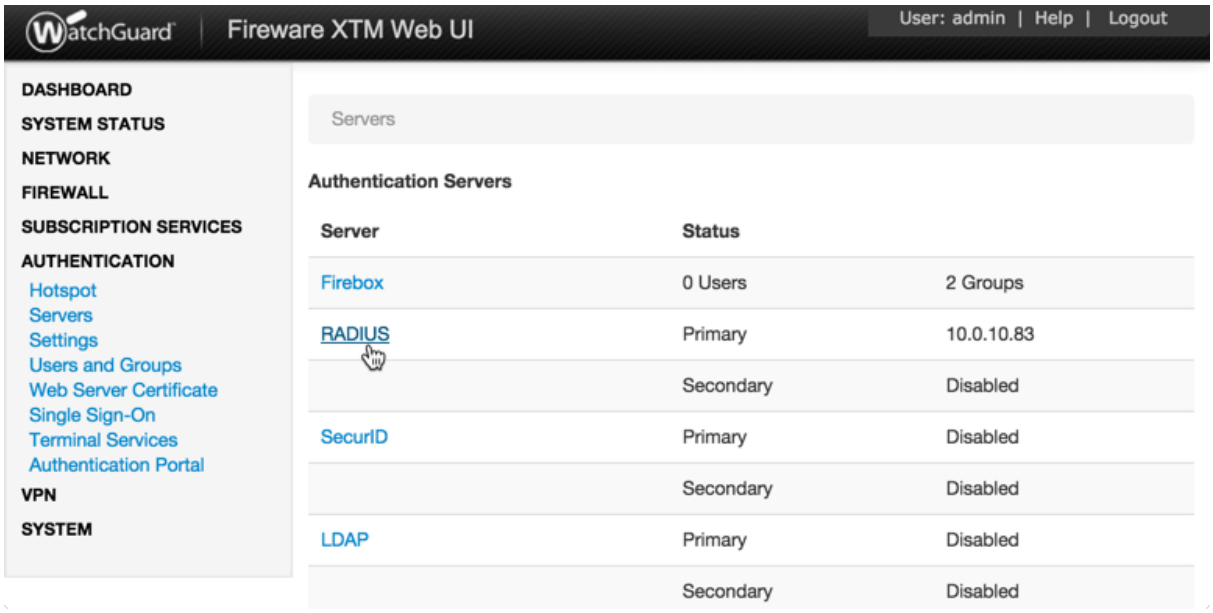
1. Select **Authentication** from the left-hand navigation bar



2. Click **Servers**

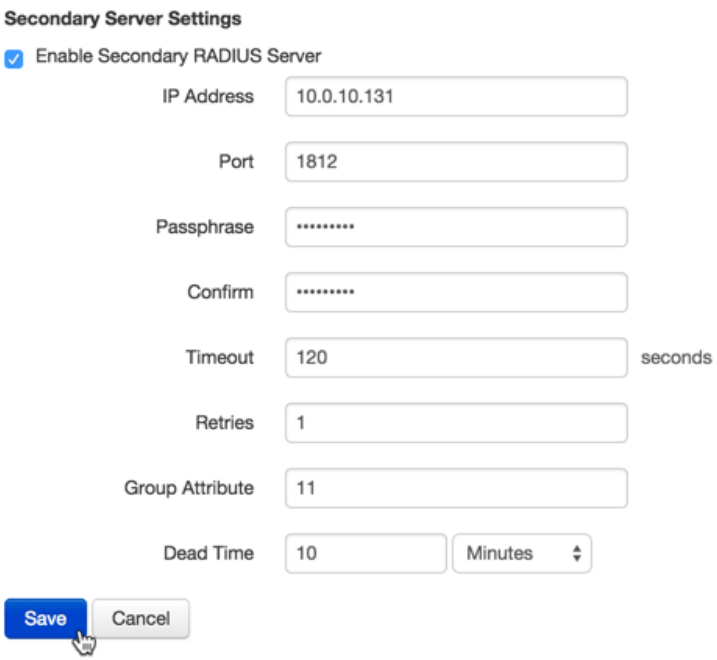


3. Select **RADIUS**



4. Check the box to **Enable Secondary RADIUS Server**

5. Complete the Secondary Server Settings Form using the same settings as the primary one



Property	Explanation	Example
`IP Address`	Address of Secondary LoginTC RADIUS Connector	10.0.10.131
`Port`	RADIUS authentication port. Must be 1812.	1812
`Passphrase`	The secret shared between the LoginTC RADIUS Connector and its client	newsecret
`Confirm`	The secret shared between the LoginTC RADIUS Connector and its client	newsecret
`Timeout`	Amount of time in seconds to wait. Must be at least 10 seconds longer than the LoginTC Request Timeout.	70
`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 an unresponsive RADIUS server is marked as inactive before the WatchGuard device attempts to connect to it again	10

6. Click **Save**

Troubleshooting

User Receives Multiple LoginTC Requests

See the Knowledge Base articles:

- My WatchGuard SSL VPN users receive multiple LoginTC requests. What can I do?
- My WatchGuard IPSec VPN users receive multiple LoginTC requests. What can I do?

Authentication times out

See the Knowledge Base articles:

- My WatchGuard SSL VPN users receive multiple LoginTC requests. What can I do?
- My WatchGuard IPSec VPN users receive multiple LoginTC requests. What can I do?

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
   ```

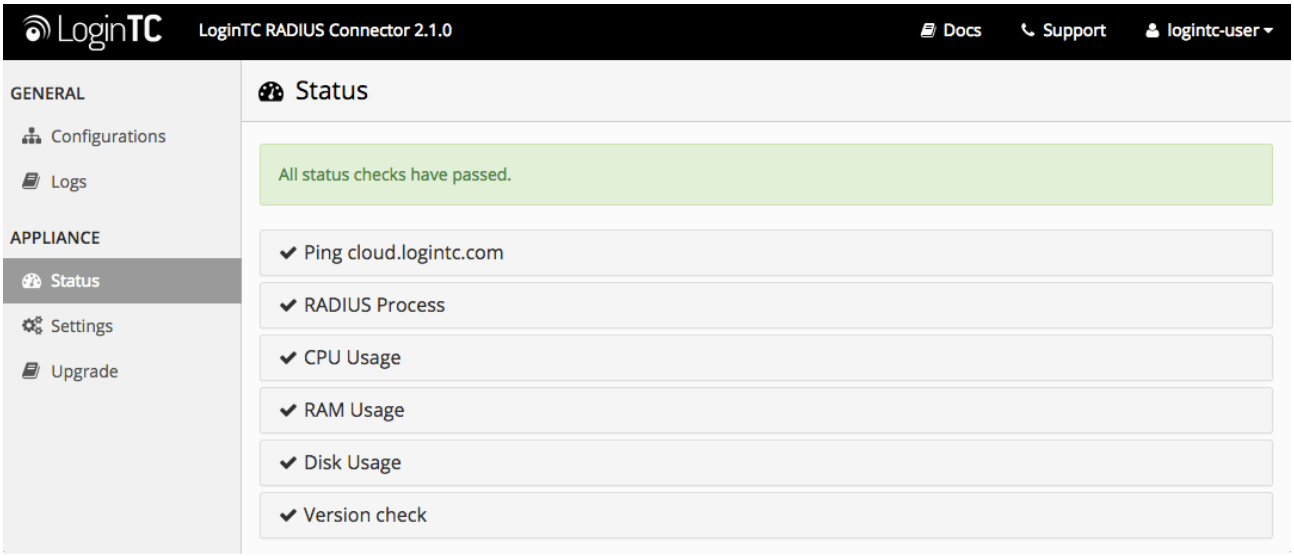
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

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

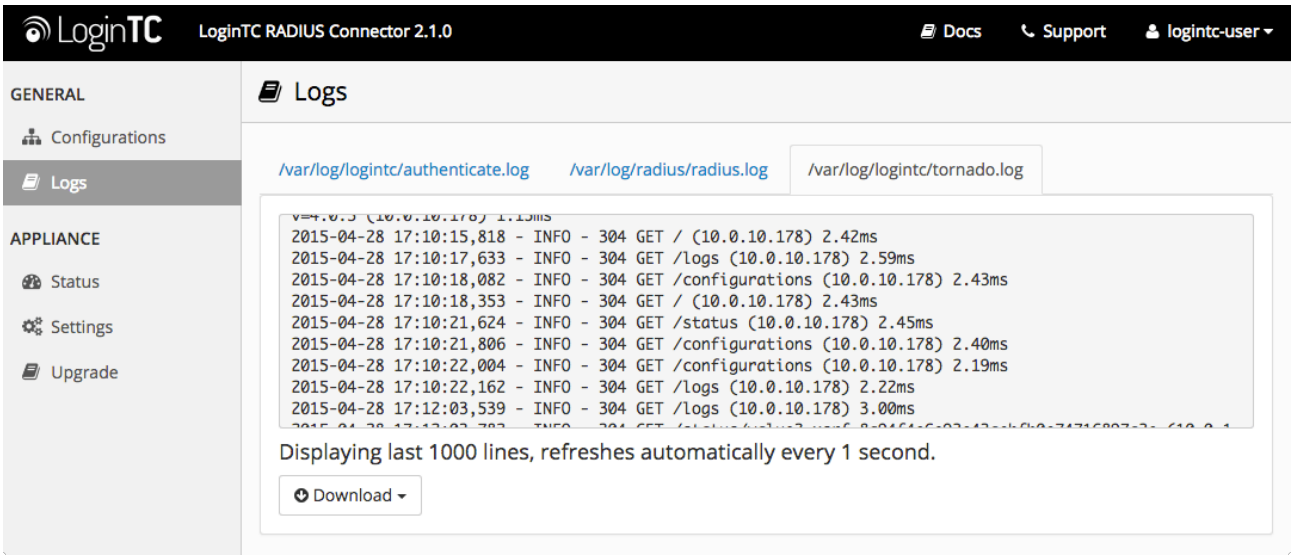
   Open the file and update the `DEVICE="eth0"` line to `DEVICE="eth1"`

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**:



Unsuccessful authentication may be caused by premature timeouts

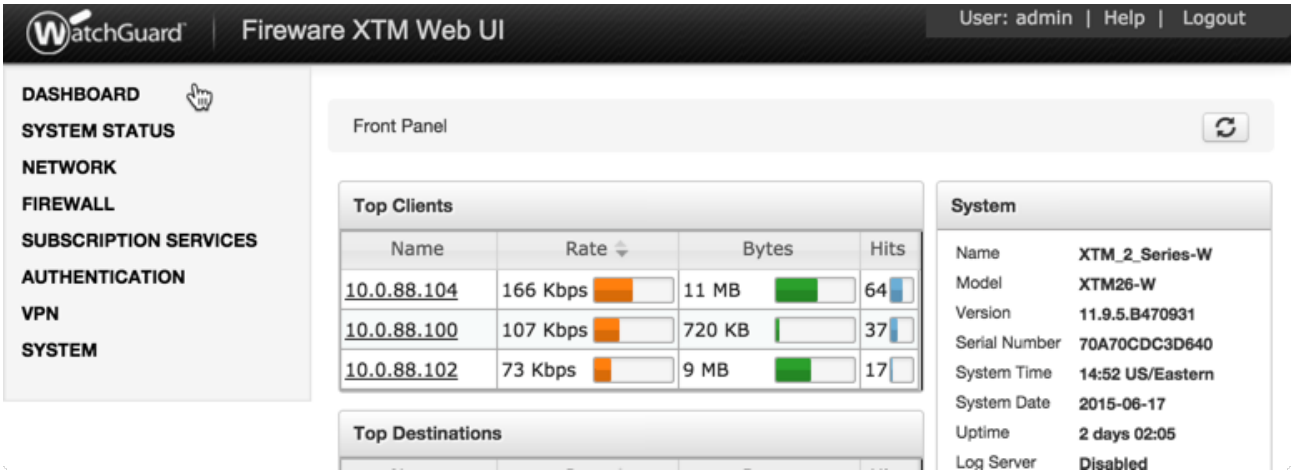
If you have activated Mobile VPN with SSL, check that your Group Attributes are configured correctly.

Email Support

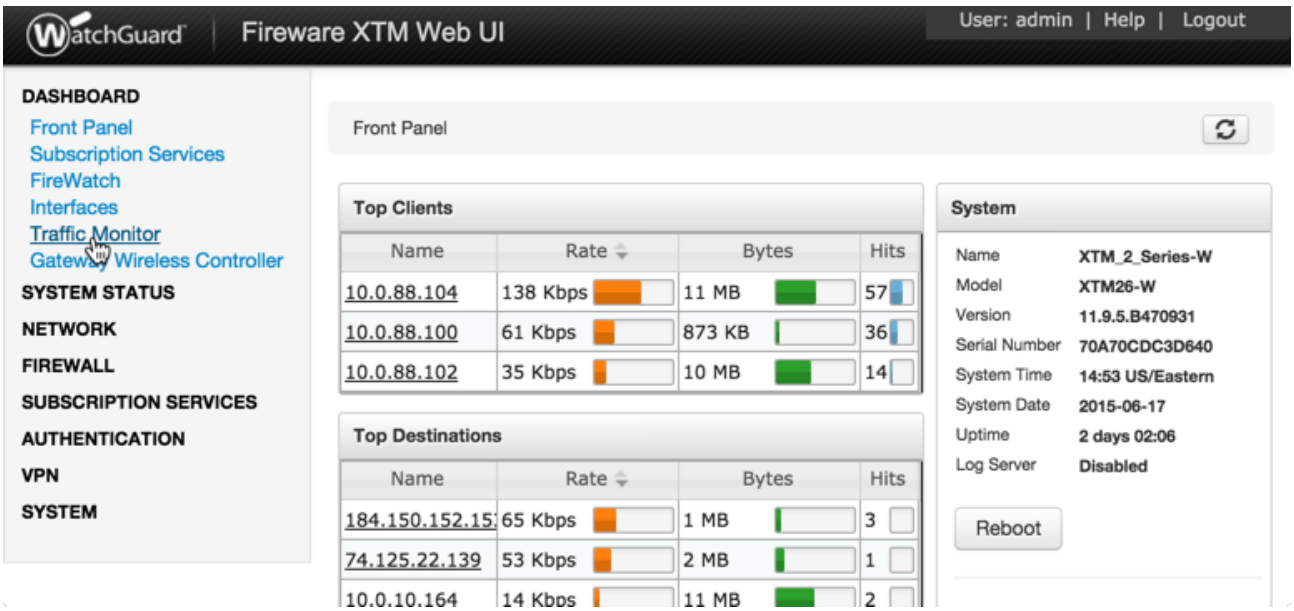
For any additional help please email support@cyphercor.com. Expect a speedy reply.

Incorrect Group Settings

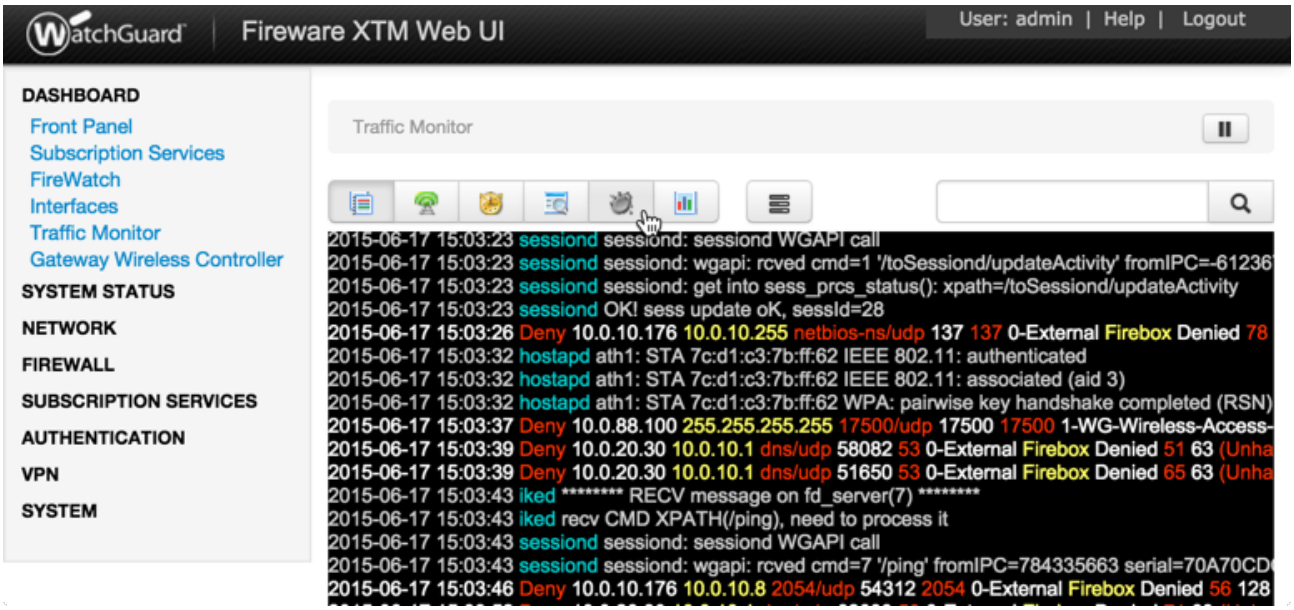
If you are using a Mobile VPN protocol such as SSL and are unable to authenticate, check that your Group Attributes are configured correctly. Navigate to your **WatchGuard Web UI** and click **Dashboard** in the left-hand navigation bar:



Click on **Traffic Monitor**:



Select **Diagnostic** from the table header options:



If you can find the following error message then there is a problem with your Group Attribute

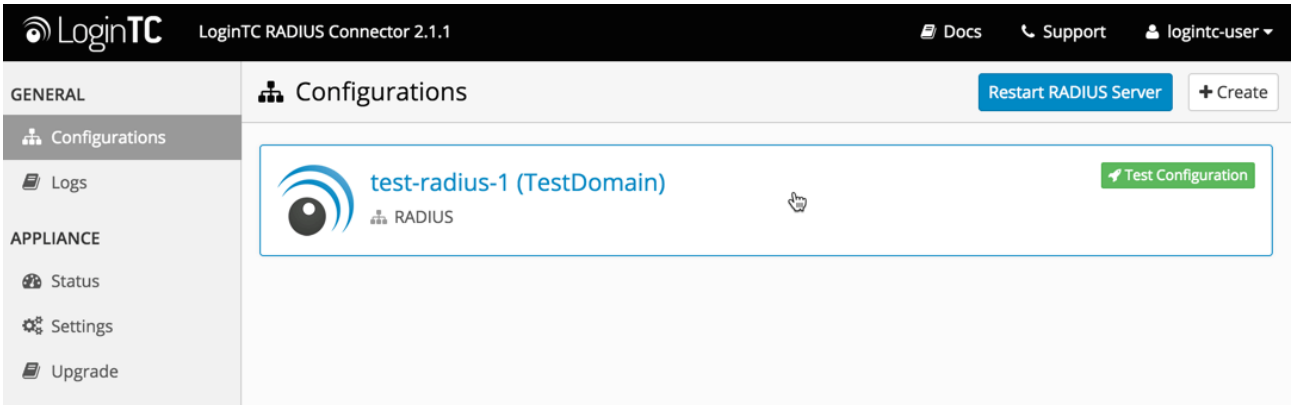
settings:

```
2015-XX-XX 16:52:41 admd Authentication failed: user username@RADIUS isn't in the authorized SSLVPN group/user list!
```

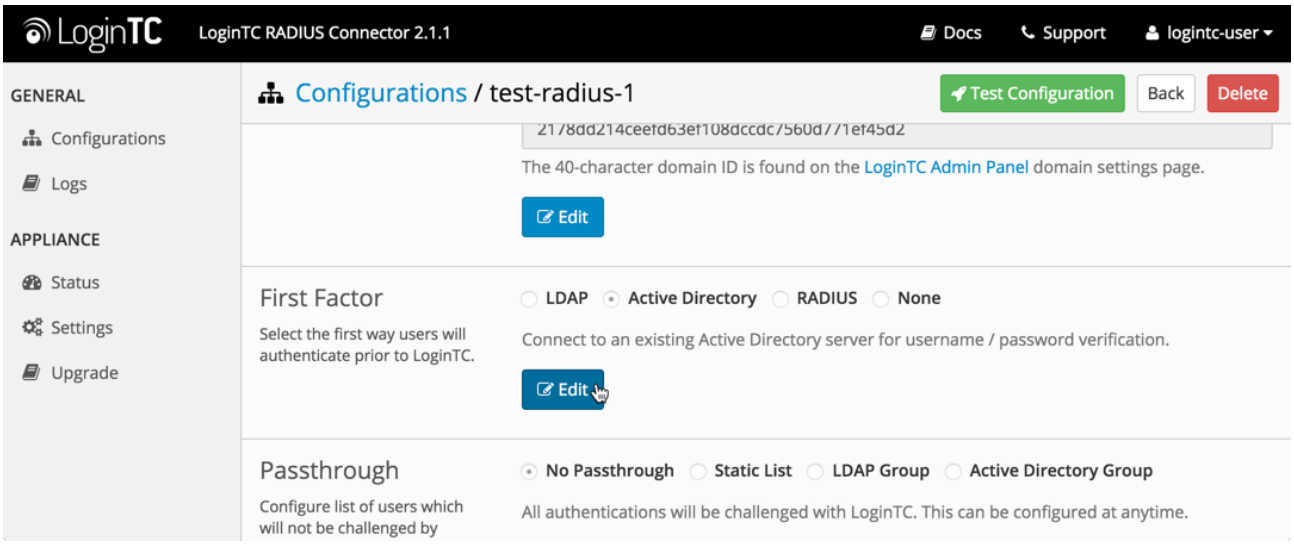
Search for the following error message:

```
2015-XX-XX 16:59:52 admd RADIUS: no attribute-value pair is retrieved from packet
```

If found, it means that the RADIUS Connector is not sending back any Group Attribute information. Navigate to your appliance **web interface** and click **Configurations**. Select the domain you're having problems with:

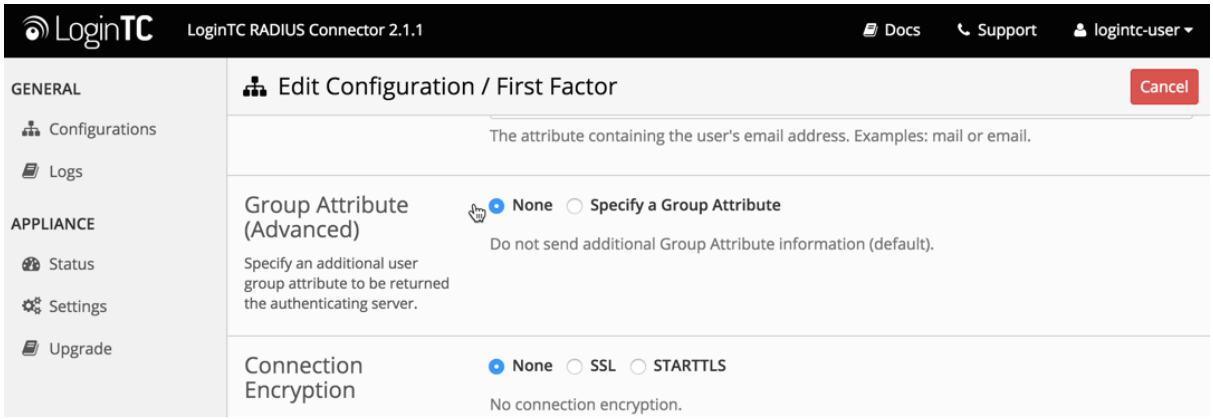


Click the **Edit Button** in the **First Factor** section:

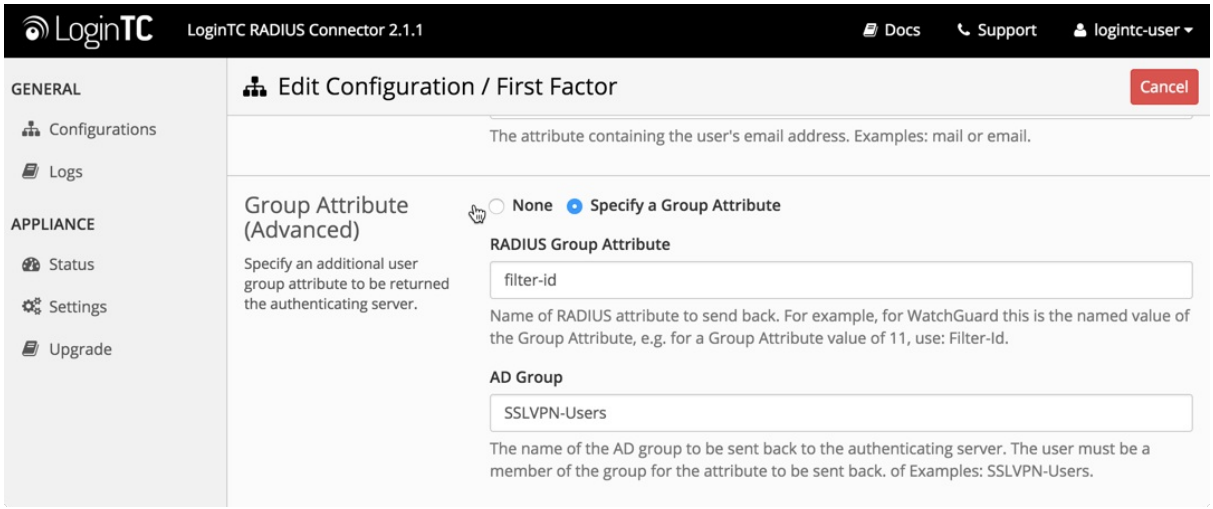


Scroll down to the to the **Group Attribute** section:

1. If "None" is selected, change it to "Specify a group attribute".Click here to review how to configure the Group Attribute for SSL



2. Otherwise, check that your user is a member of the specified group in the LDAP Directory. If they are not, it will cause RADIUS to return a blank attribute.

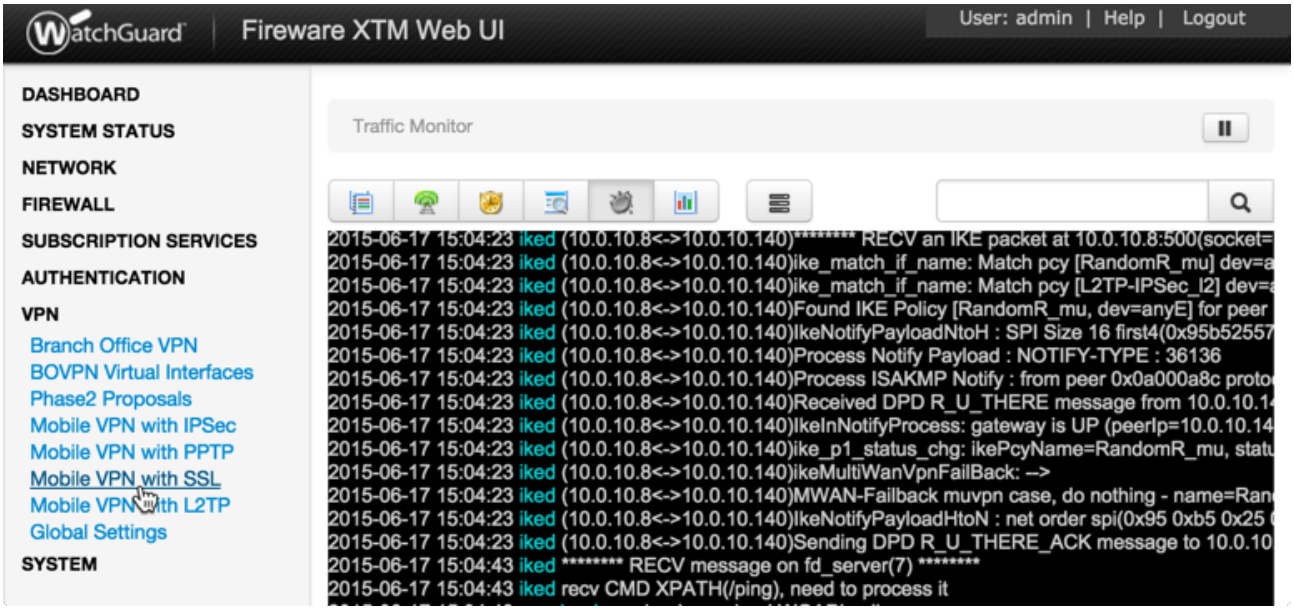


If you find a log message similar to this:

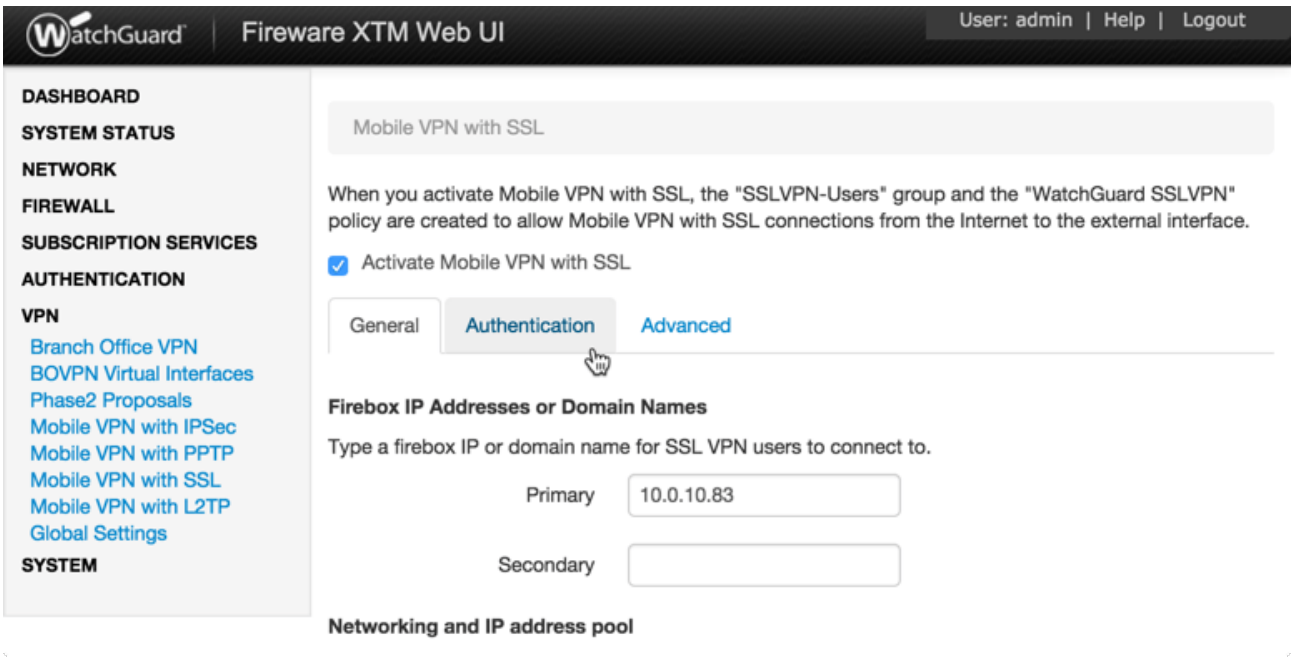
```
2015-XX-XX 16:52:41 admd RADIUS: finished parsing attribute-value pairs
2015-XX-XX 16:52:41 admd RADIUS: group 1, type=11 value=L2TP-Users
2015-XX-XX 16:52:41 admd RADIUS: retrieve VP:Filter-Id(11) int=10
```

Then the RADIUS server is sending back a Group Attribute, but it may not be the correct one.

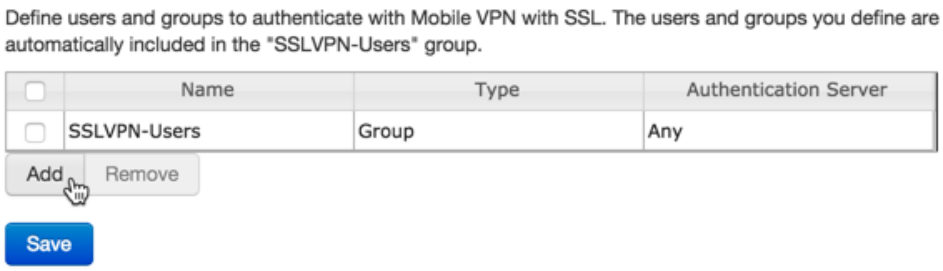
Check that the **value** is the name of the group that has been added to list of groups authorized to authenticate with SSL. Log into the **WatchGuard Web UI** and select **VPN** from the left-hand navigation bar. Click on **Mobile VPN with SSL** :



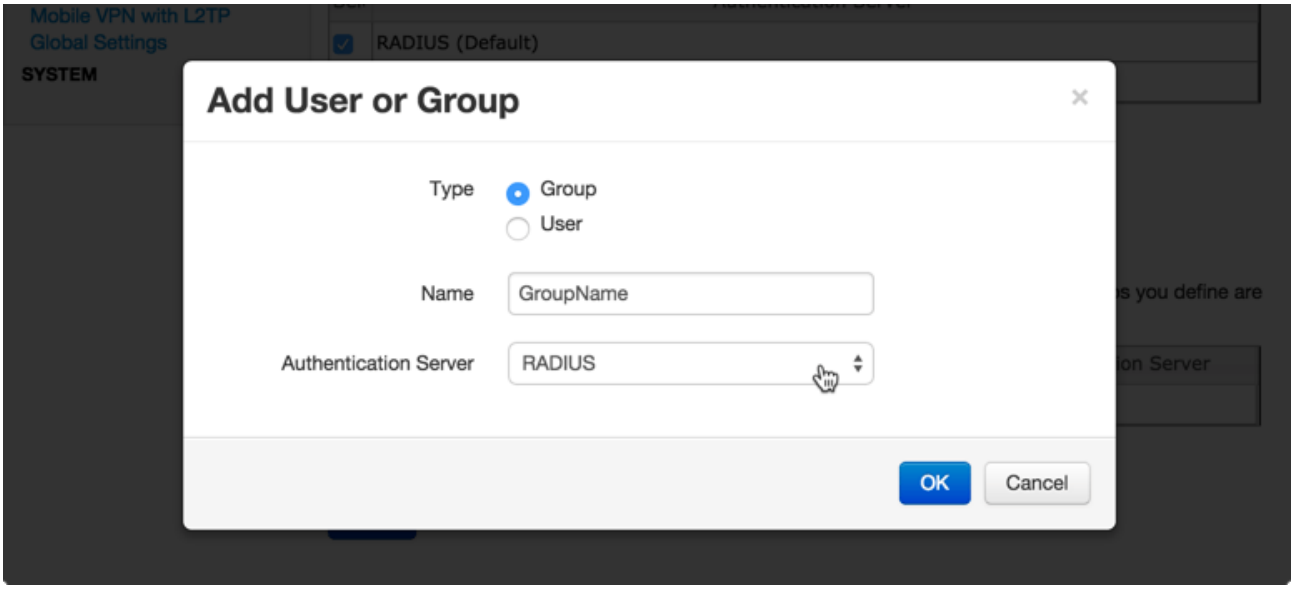
Click on the **Authentication** tab:



The bottom table contains the list of groups that are authorized to connect with SSL. If the group returned by the RADIUS server is not part of it, it must be added. Click the **Add** button:

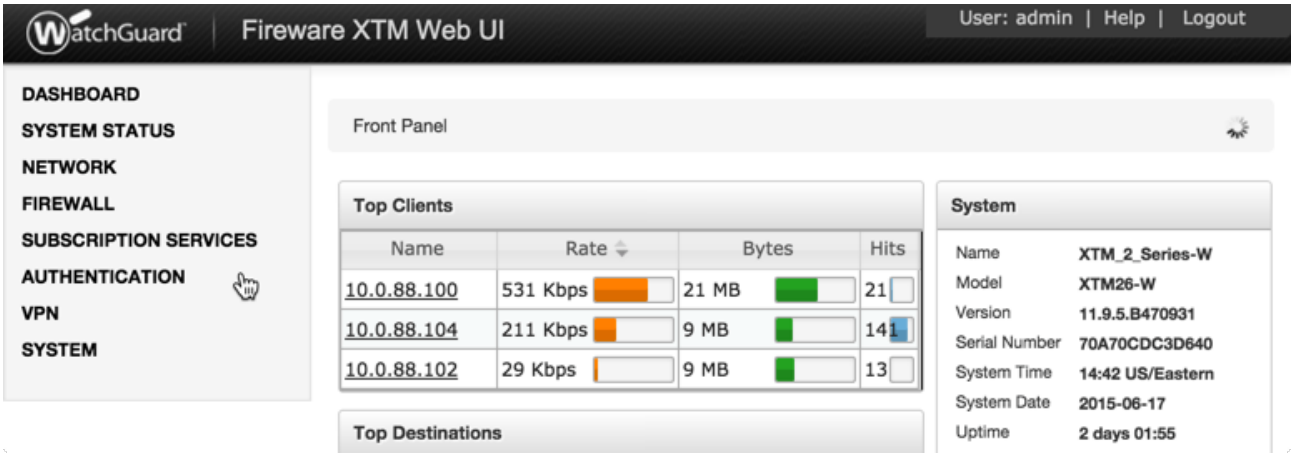


Type in the group name and select **RADIUS** as the Authentication Server:

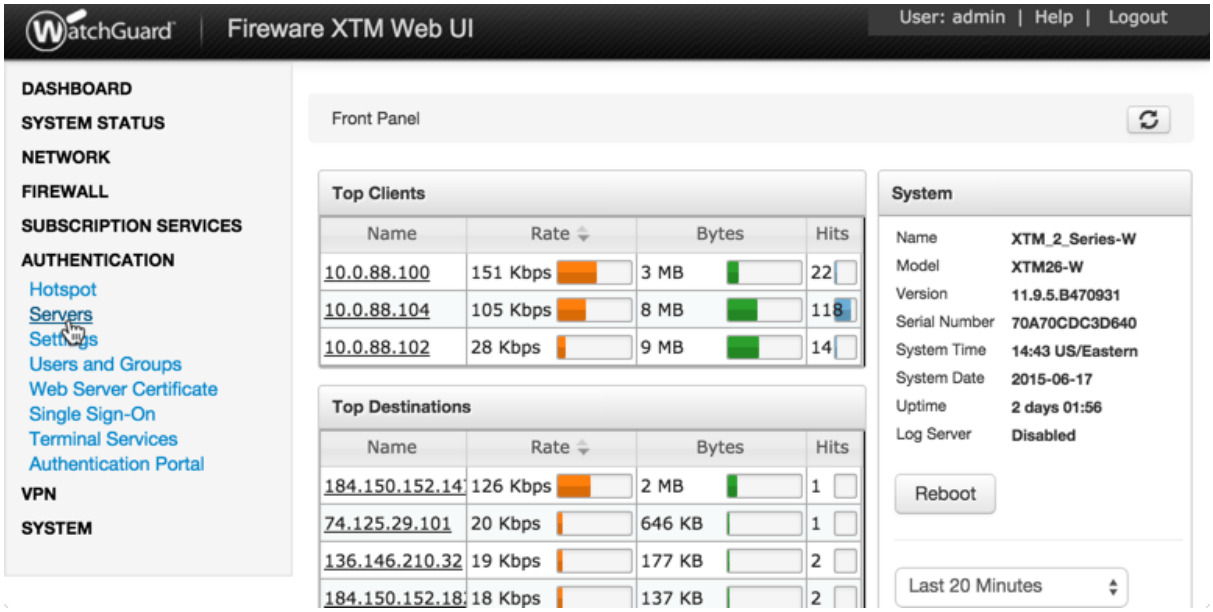


Authentication Timing Out

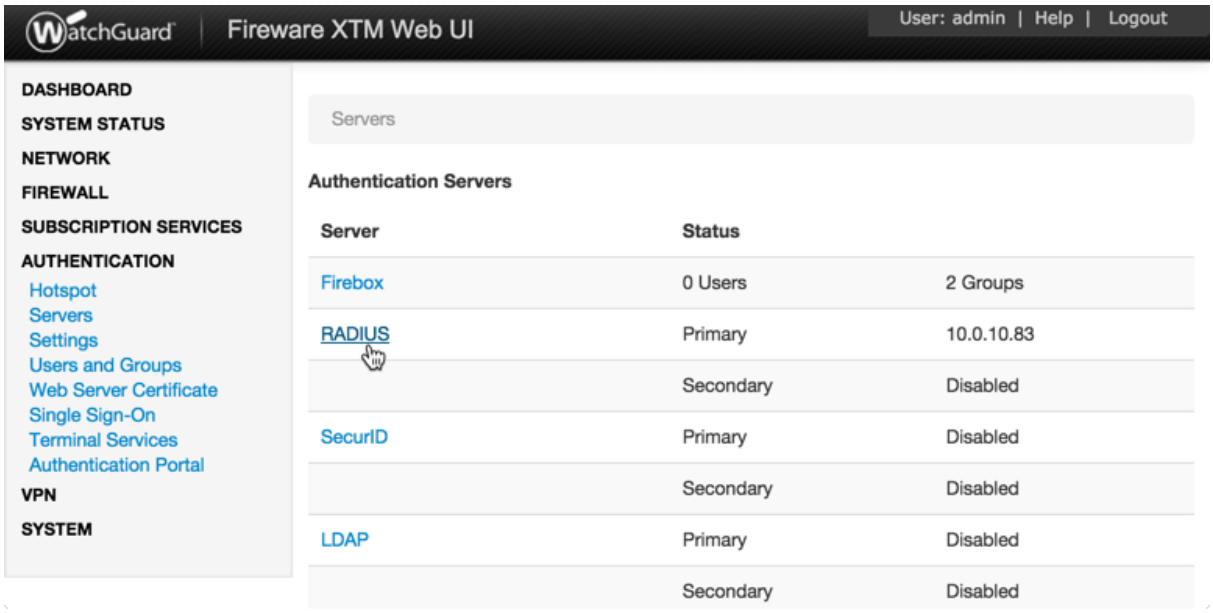
If authentication is failing, it is possible that the authentication requests are timing out too quickly. By default, LoginTC push requests will timeout after 90 seconds. Another timeout value is defined by the RADIUS server configuration. If it is set too low, it will cause requests to prematurely timeout. To check, login to your **WatchGuard Web UI**



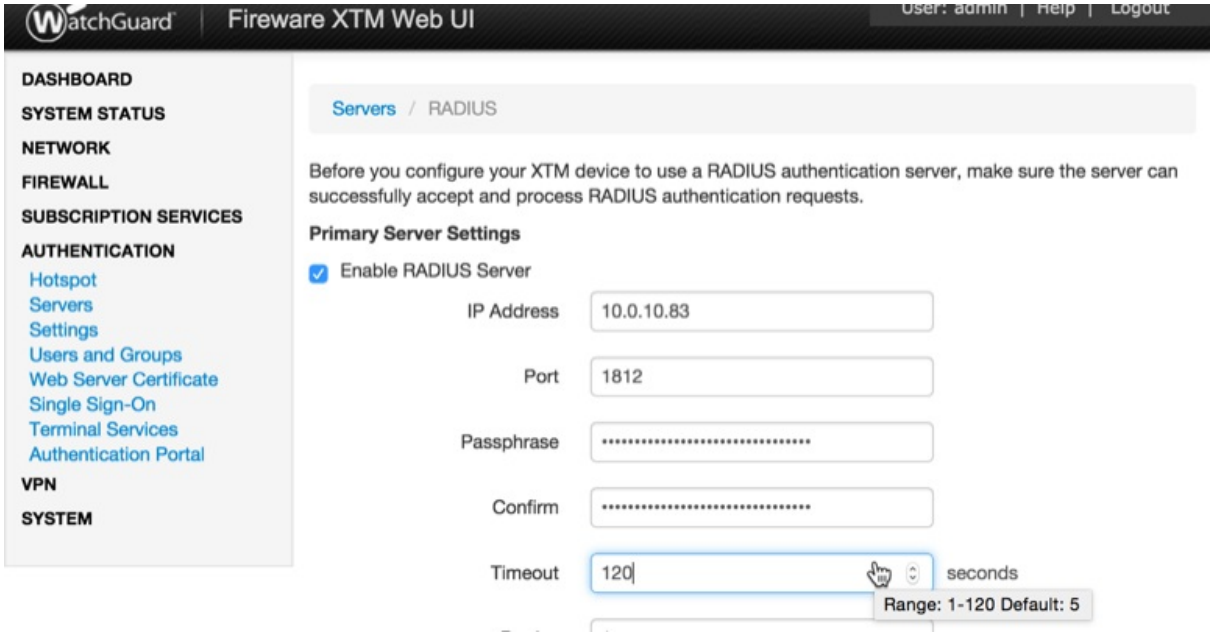
1. Select **Authentication** from the left-hand navigation bar, then click **Servers**



2. Click **RADIUS**



3. Check the **Timeout** attribute field. It should be at least 10 seconds longer than the LoginTC Request Timeout set in the LoginTC RAIDUS Connector.



See the Knowledge Base articles for more information:

- My WatchGuard SSL VPN users receive multiple LoginTC requests. What can I do?
- My WatchGuard IPSec VPN users receive multiple LoginTC requests. What can I do?
