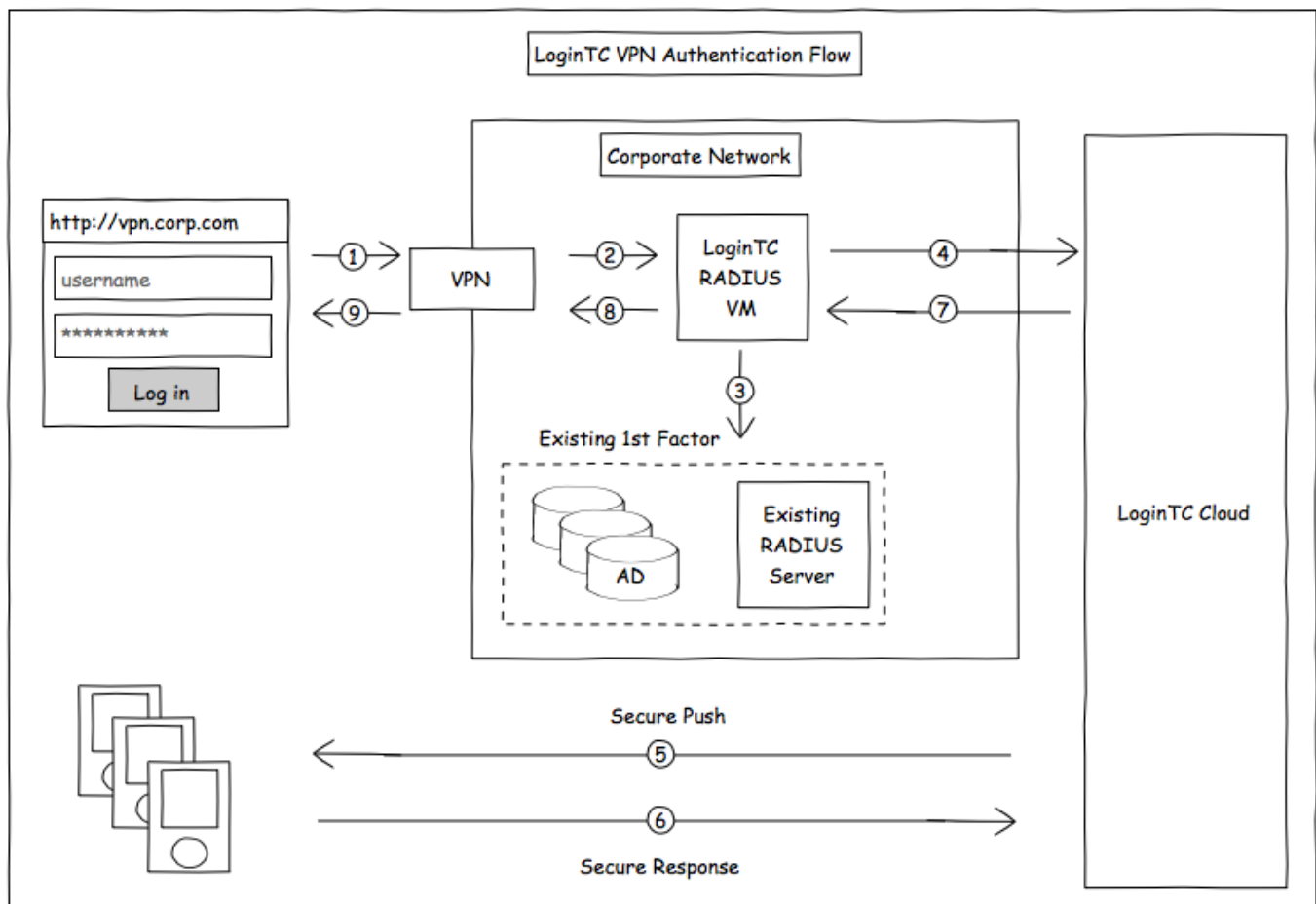


Two factor authentication for WatchGuard XTM and Firebox

logintc.com/docs/connectors/watchguard-ssl.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 the [WatchGuard XTM](#) and Firebox VPN (e.g. Mobile VPN with SSL or IPsec) 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. For example, WatchGuard Mobile VPN with SSL.

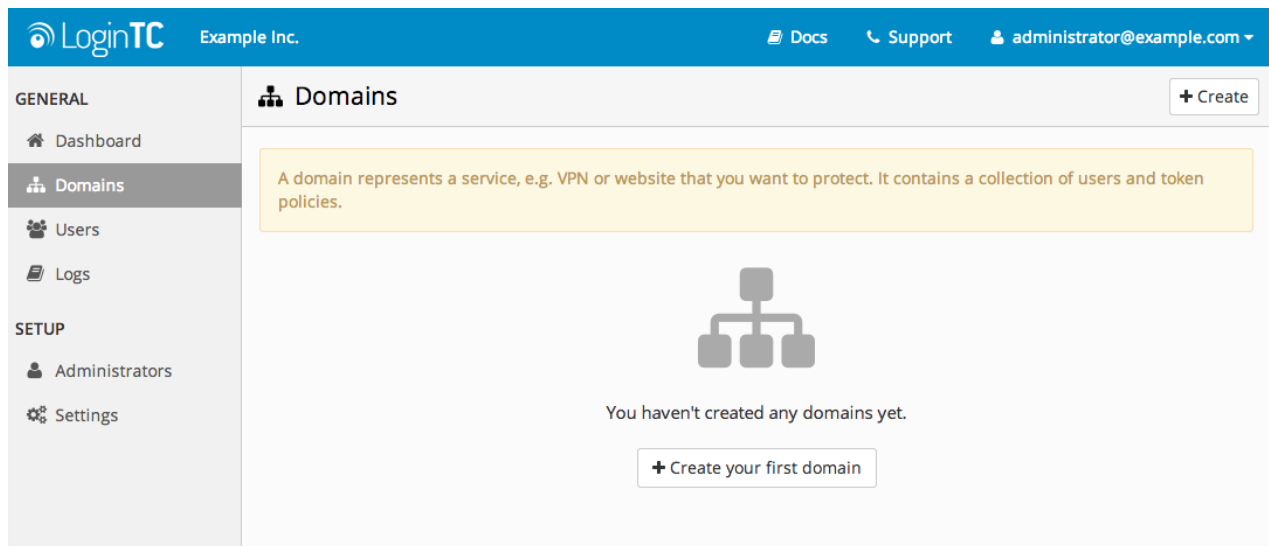
Prerequisites

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:

GENERAL


- Dashboard
- Domains**
- Users
- Logs

SETUP

- Administrators
- Settings

Domains / Create Domain Cancel

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

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


Connector
How you will connect your infrastructure to this domain
 RADIUS API OpenAM SiteMinder Drupal WordPress Joomla
RADIUS
 Use the RADIUS Connector for your RADIUS appliance

Key Policy
Specify how your users will unlock their token to authenticate
 PIN Passcode
 Note: if you are already using passwords for the first factor, we recommend PIN

Create

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

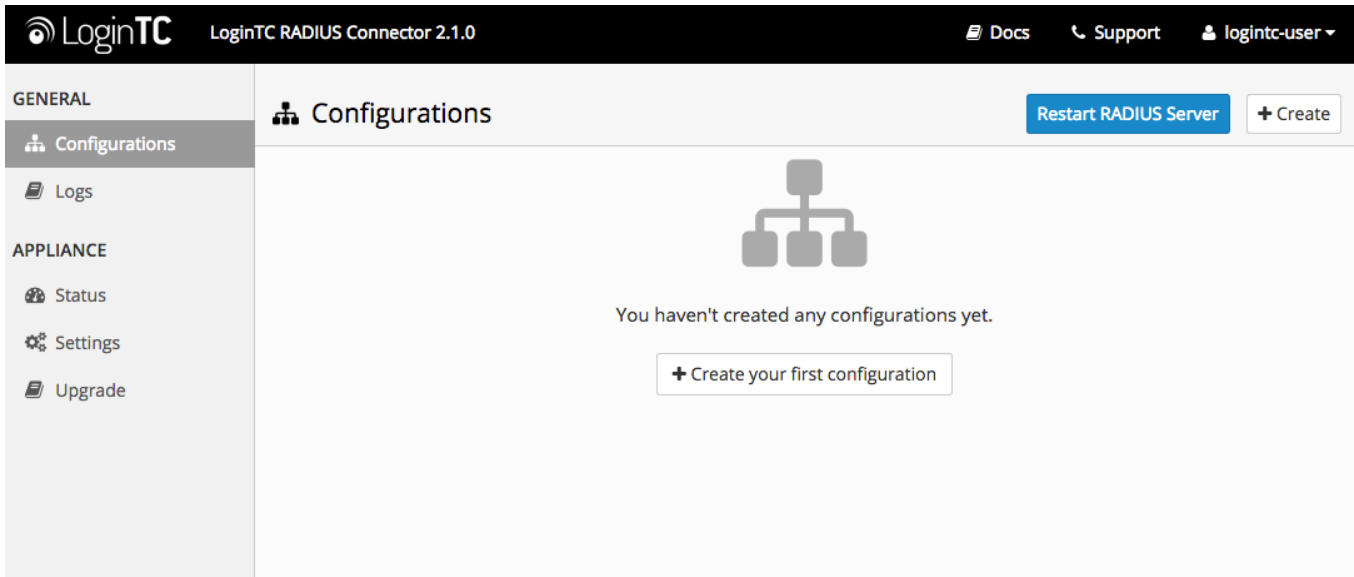
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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

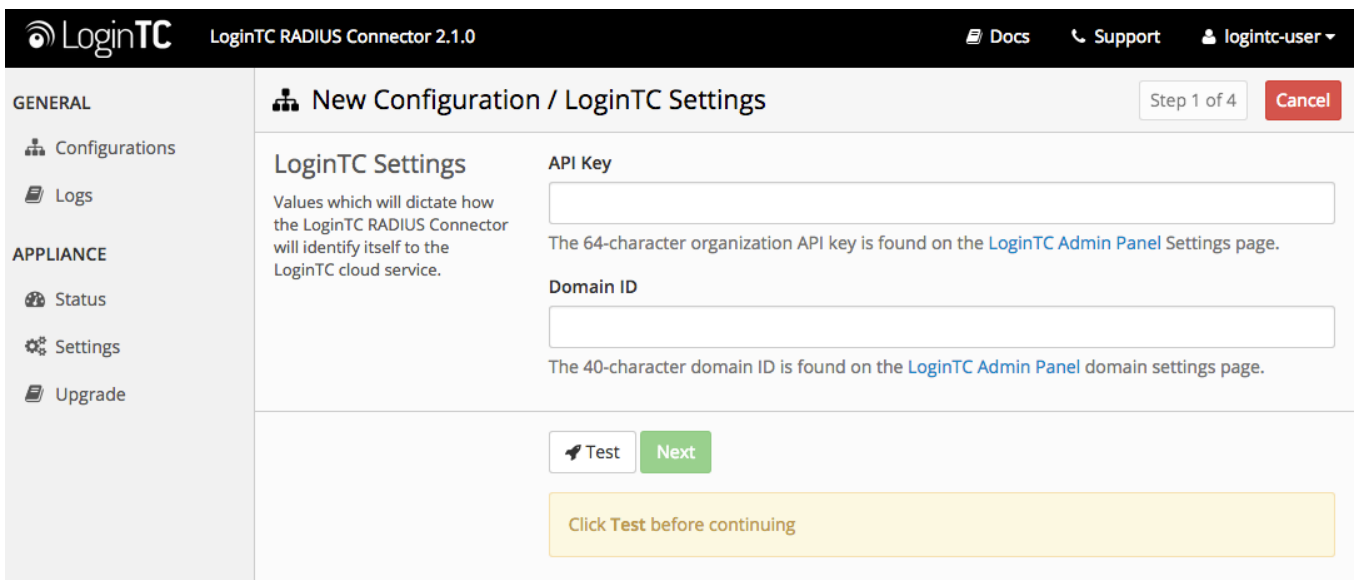
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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**:


LoginTC RADIUS Connector 2.1.0

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

GENERAL

- Configurations
- Logs

APPLIANCE

- Status
- Settings
- Upgrade

Step 1 of 4
Cancel

New Configuration / LoginTC Settings

LoginTC Settings

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

API Key

vZkDw7l6Z3tApwZjXERseKdR0s5RNNqjMxXlwvxpWwjOa9oJXI9b5tdvPyFsqzWj

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

Select the first way users will authenticate prior to LoginTC.

LDAP
 Active Directory
 RADIUS
 None

Connect to an existing LDAP server for username / password verification.

LDAP Server Details

The LDAP host and port information.

Host

Host name or IP address of the LDAP server. Examples: ldap.example.com or 192.168.1.42

Port (optional)

389

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 LoginTC RADIUS Connector 2.1.0 Docs Support loginc-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

The Active Directory host and port information.

Host

Host name or IP address of the LDAP server. Examples: ad.example.com or 192.168.1.42

Port (optional)

Port if Active Directory server uses non-standard port.

Bind Details Bind with credentials Anonymous

Configuration values:

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

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

Group Attribute and Access Control

In order to use Mobile VPN with SSL, 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.

To match WatchGuard's default values, set **RADIUS Group Attribute** to `Filter-Id` and **LDAP Group** to `SSLVPN-Users`

LDAP Group / AD Group : The name of a group in the LDAP Directory that all authenticating users belong to. The group name must also be added to WatchGuard's list of groups authorized to authenticate using SSL. By default this is only the SSLVPN-Users group, but other groups can be added manually from the WatchGuard Web UI.

The screenshot shows the LoginTC RADIUS Connector 2.1.0 web interface. The main heading is "New Configuration / First Factor" with a "Step 2 of 4" indicator and a "Cancel" button. The left sidebar shows "GENERAL" with "Configurations" selected, and "APPLIANCE" with "Status", "Settings", and "Upgrade" options. The main content area is titled "Group Attribute (Advanced)" and includes the instruction: "Specify an additional user group attribute to be returned the authenticating server." There are two radio buttons: "None" (unselected) and "Specify a Group Attribute" (selected). Under "RADIUS Group Attribute", there is a text input field containing "Filter-Id" and a descriptive note: "Name of RADIUS attribute to send back. For example, for WatchGuard this is the named value of the Group Attribute, e.g. for a Group Attribute value of 11, use: Filter-Id." Below that, there is an empty text input field for "LDAP Group" with a note: "The name of the LDAP group to be sent back to the authenticating server. The user must be a member of the group for the attribute to be sent back. of Examples: SSLVPN-Users."

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, 192.168.1.43</code>
<code>port (optional)</code>	Port if the RADIUS server uses non-standard (i.e., <code>1812</code>)	<code>6812</code>
<code>secret</code>	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	<code>testing123</code>

RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) found in the FreeRADIUS dictionary files will be relayed.

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

Passthrough

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

For example, with smaller or proof of concept deployments select the [Static List](#) option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured [First Authentication Factor](#). That means you will be able to test LoginTC without affecting existing users accessing your VPN.

For larger deployments you can elect to use the [Active Directory or LDAP Group](#) option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC your LDAP and Active Directory group policy will ensure that they will be challenged with LoginTC. Users not part of the group will only be challenged with the configured [First Authentication Factor](#).

No Passthrough (default)

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

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

Static List

Select this option if you wish to have a static list of users that will be challenged with LoginTC. Good for small number of users.

The screenshot shows the LoginTC configuration interface for 'New Configuration / Passthrough' at 'Step 3 of 4'. The 'Static List' radio button is selected. The text below the options reads: '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.' Below this, there is a section titled 'Static List' with the text: 'Only users in this list will be challenged with LoginTC. All other users will be challenged with configured first factor only.' To the right of this text is a large empty text area labeled 'LoginTC challenge users' for entering a list of usernames.

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

```
jane.doe  
jane.smith  
john.doe  
john.smith
```

Active Directory / LDAP Group

Select this option if you wish to have only users part of a particular Active Directory or LDAP group to be challenged with LoginTC. Good for medium and large number of users.

Configuration values:

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

<code>cert</code> (optional)	Certificate file (PEM format)	<code>/opt/logintc/cert.pem</code>
<code>key</code> (optional)	Key file (PEM format)	<code>/opt/logintc/key.pem</code>

Configuration Simplified

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

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

Client and Encryption

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

Client configuration values:

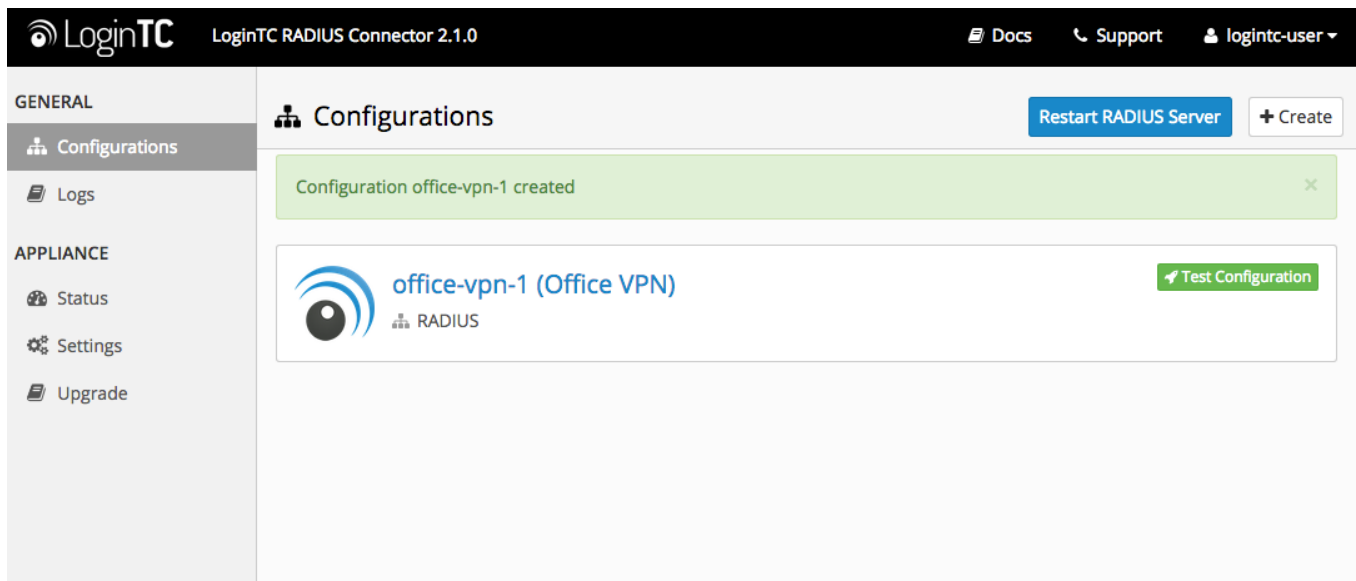
<code>name</code>	A unique identifier of your RADIUS client	<code>CorporateVPN</code>
<code>ip</code>	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	<code>192.168.1.44</code>
<code>secret</code>	The secret shared between the LoginTC RADIUS Connector and its client	<code>bigsecret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

Data Encryption

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

general best practice.

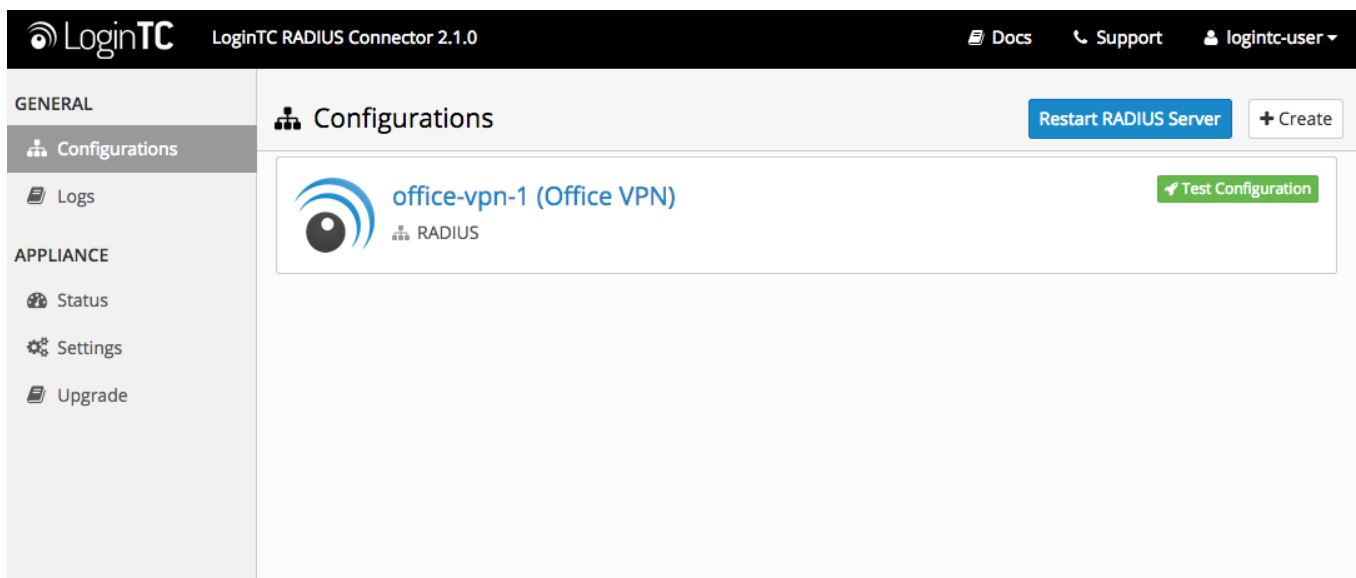
Click **Test** to validate the values and then click **Save**.



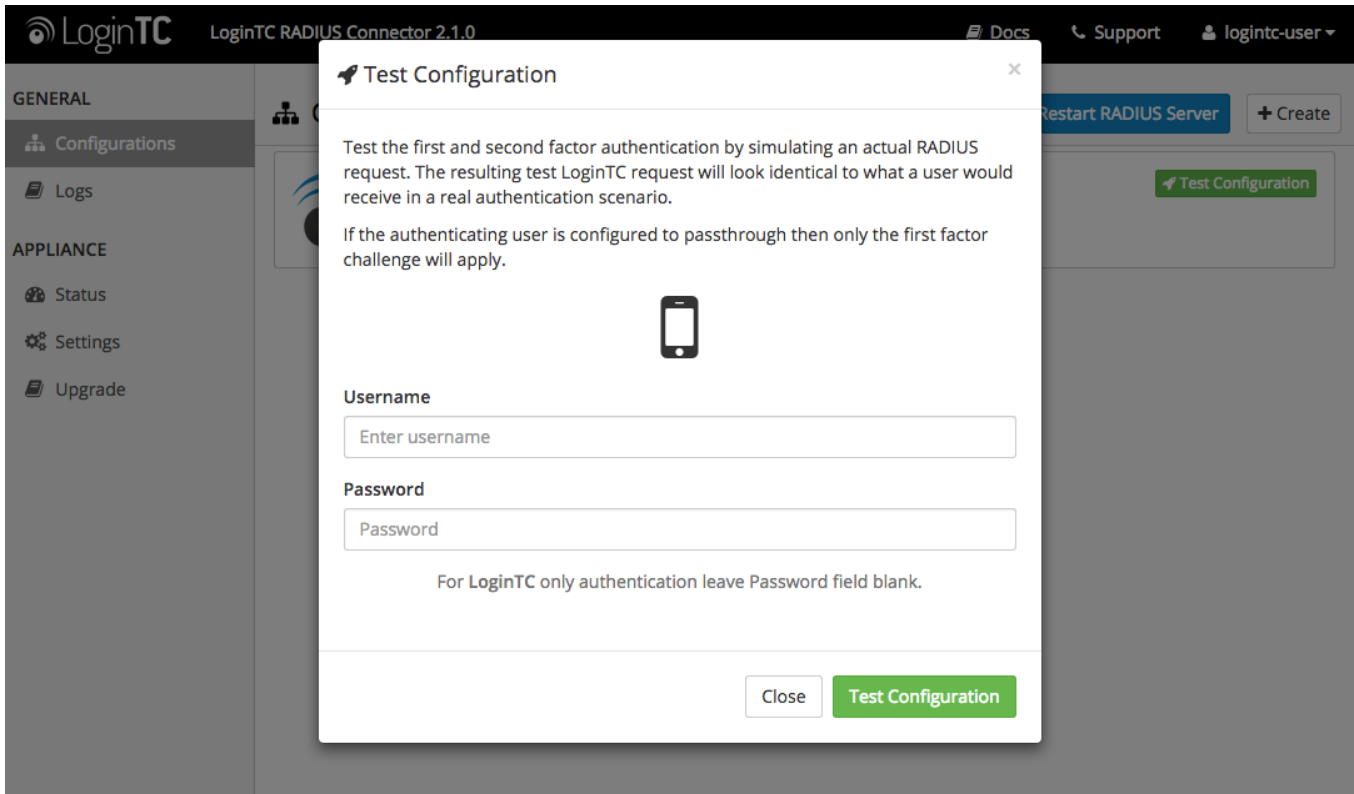
Testing (Connector)

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:

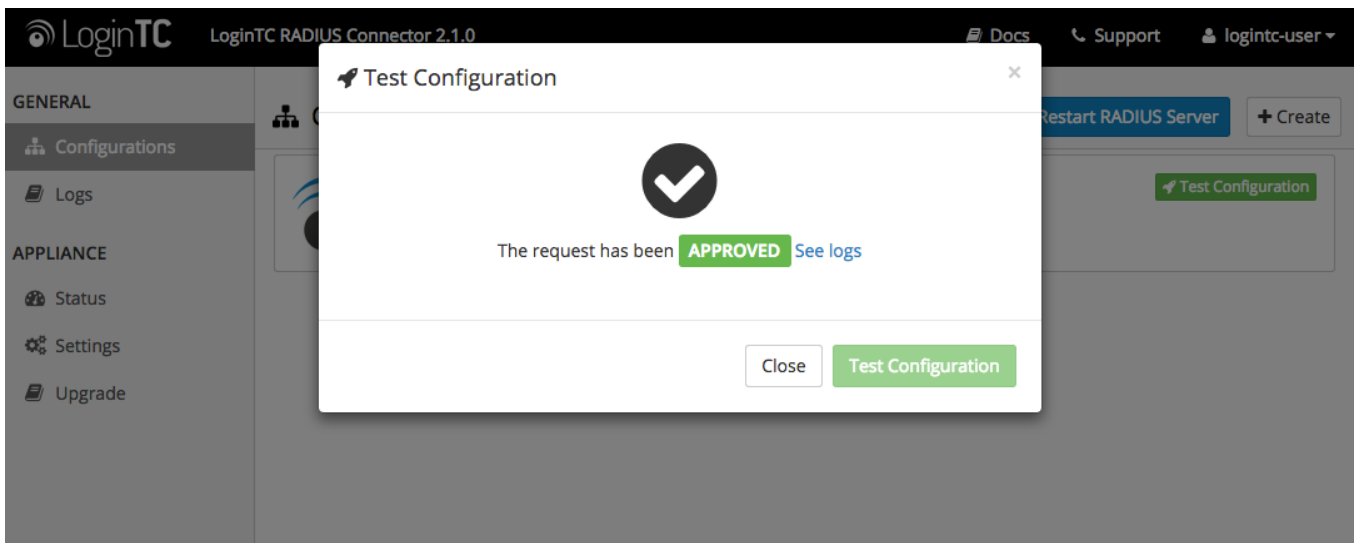
When you have loaded a token for your new user and domain, navigate to your appliance **web interface URL**:



Click **Test Configuration**:

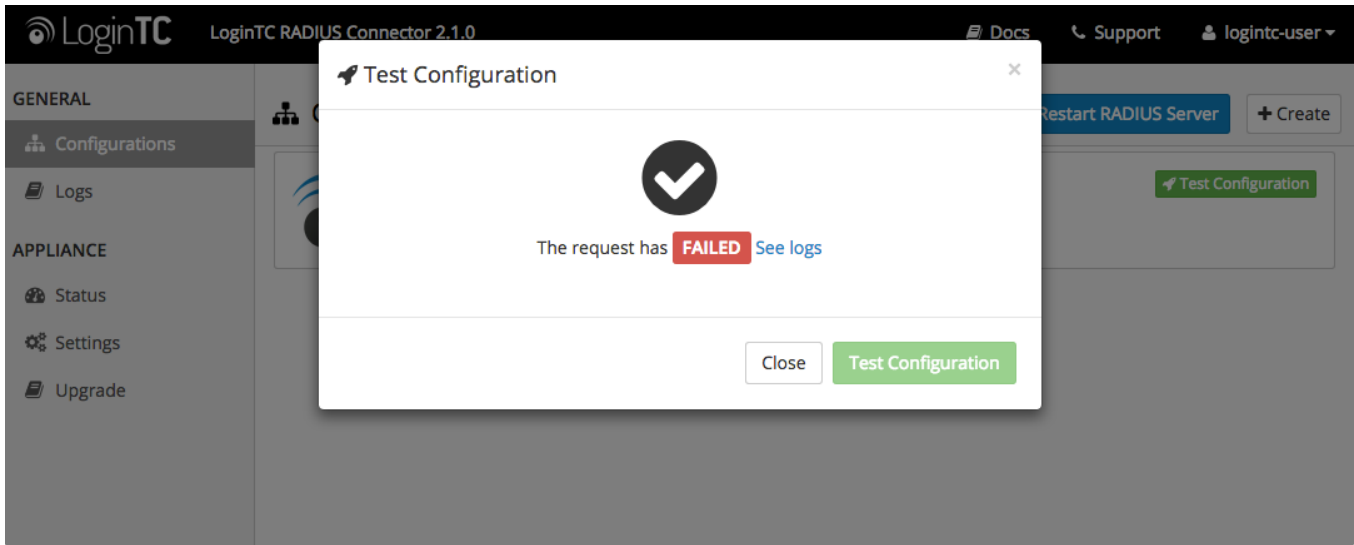


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

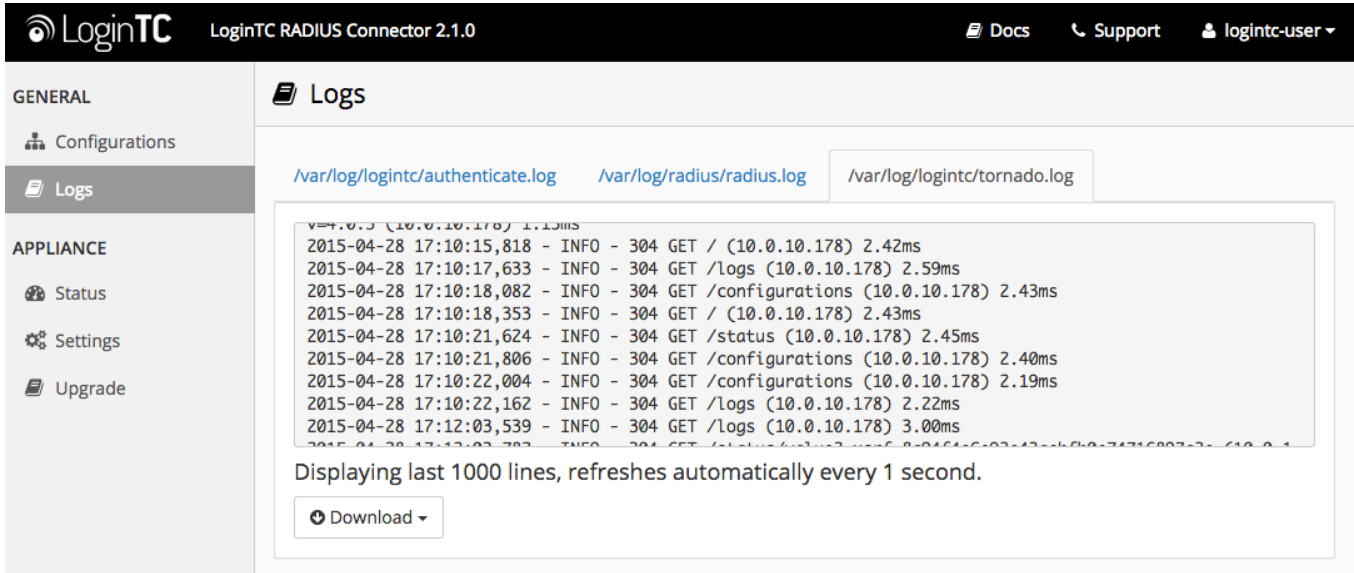


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



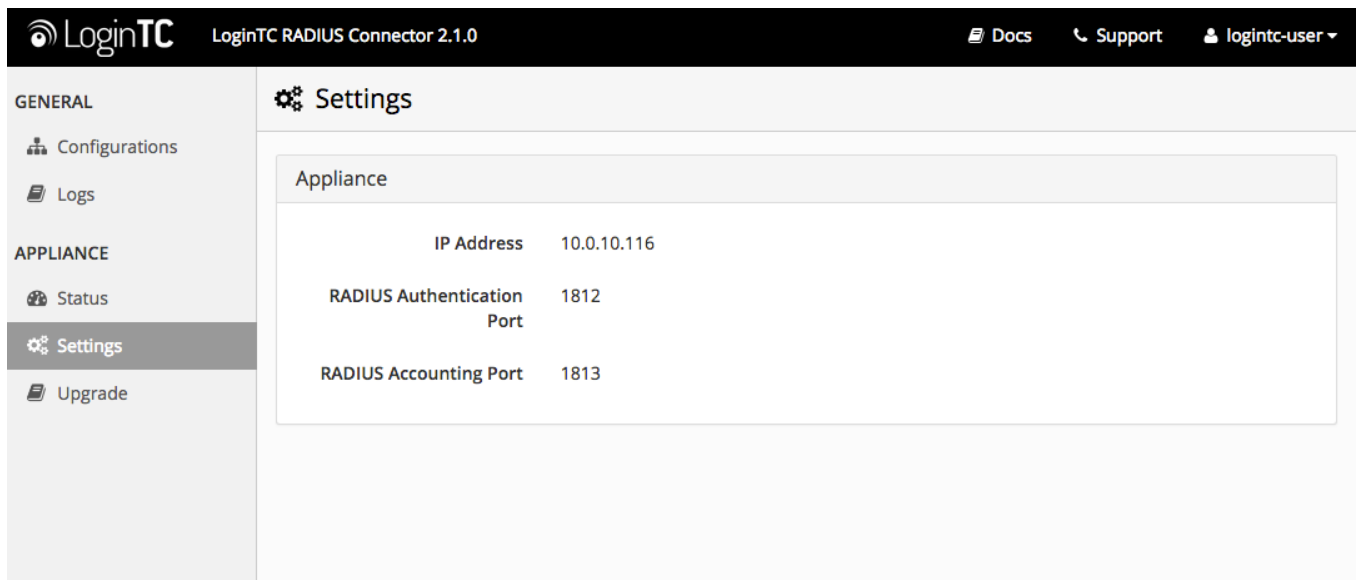
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:



WatchGuard Configuration - Quick Guide

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

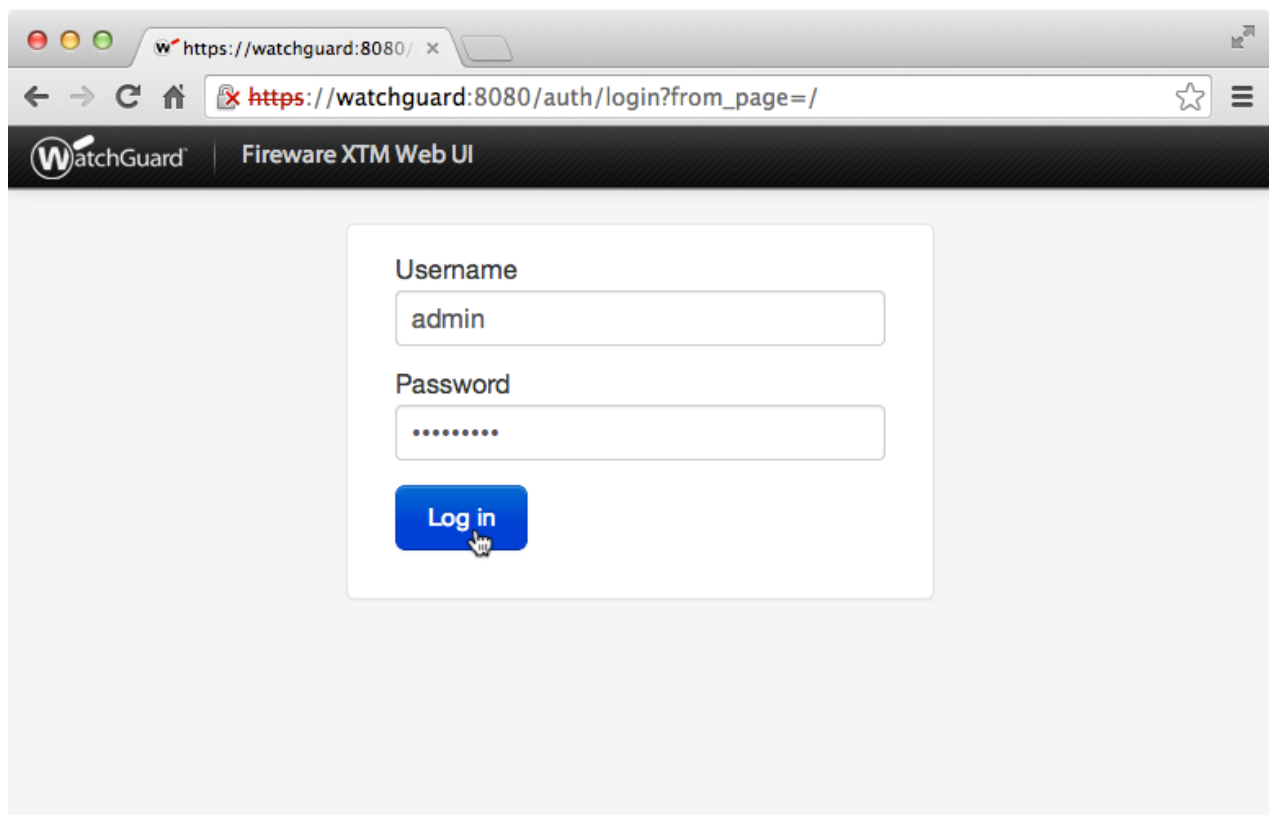
For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:



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, the same is true for other devices in the XTM series.

Mobile VPN Protocol with SSL

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



2. Click **Authentication:**

Front Panel

Top Clients			
Name	Rate	Bytes	Hits
10.0.1.5	150 Kbps	341 KB	17
10.0.10.178	13 Kbps	1 KB	1

Top Destinations			
Name	Rate	Bytes	Hits
23.60.247.88	109 Kbps	142 KB	6
173.194.43.111	19 Kbps	113 KB	1
10.0.10.183	13 Kbps	1 KB	1
23.61.177.207	7 Kbps	9 KB	1
184.150.152.18	6 Kbps	52 KB	2
63.140.54.90	3 Kbps	3 KB	1

System

Name: XTMv
 Model: XTMv
 Version: 11.8.B432340
 Serial Number: V1C500000000
 System Time: 12:48 US/Eastern
 System Date: 2013-12-13
 Uptime: 0 days 00:14
 Log Server: Disabled

Reboot

Last 20 Minutes

External Bandwidth

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

Front Panel

Top Clients			
Name	Rate	Bytes	Hits
10.0.10.178	13 Kbps	1 KB	1
10.0.1.5	4 Kbps	58 KB	3

Top Destinations			
Name	Rate	Bytes	Hits
10.0.10.183	13 Kbps	1 KB	1
184.150.152.18	2 Kbps	48 KB	1
66.196.113.5	1 Kbps	4 KB	1
173.192.82.194	208 bps	6 KB	1

System

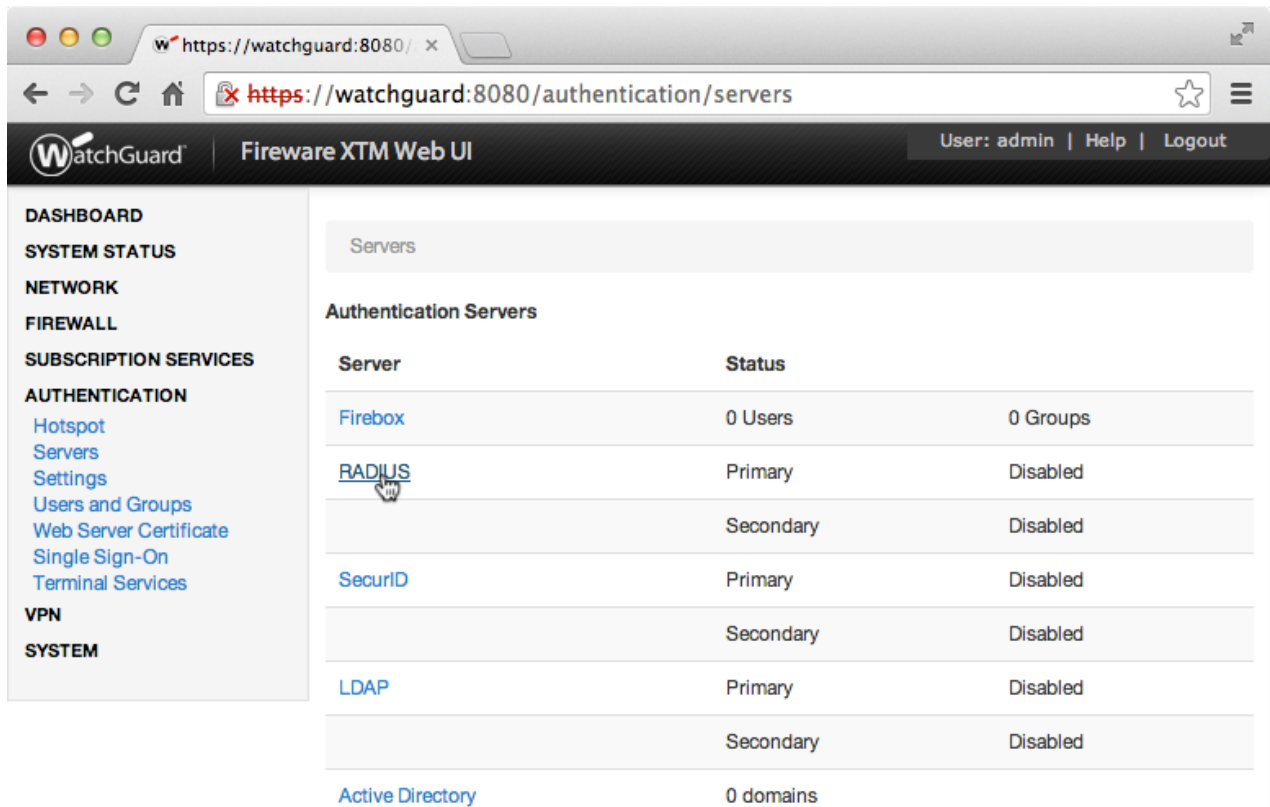
Name: XTMv
 Model: XTMv
 Version: 11.8.B432340
 Serial Number: V1C500000000
 System Time: 12:50 US/Eastern
 System Date: 2013-12-13
 Uptime: 0 days 00:16
 Log Server: Disabled

Reboot

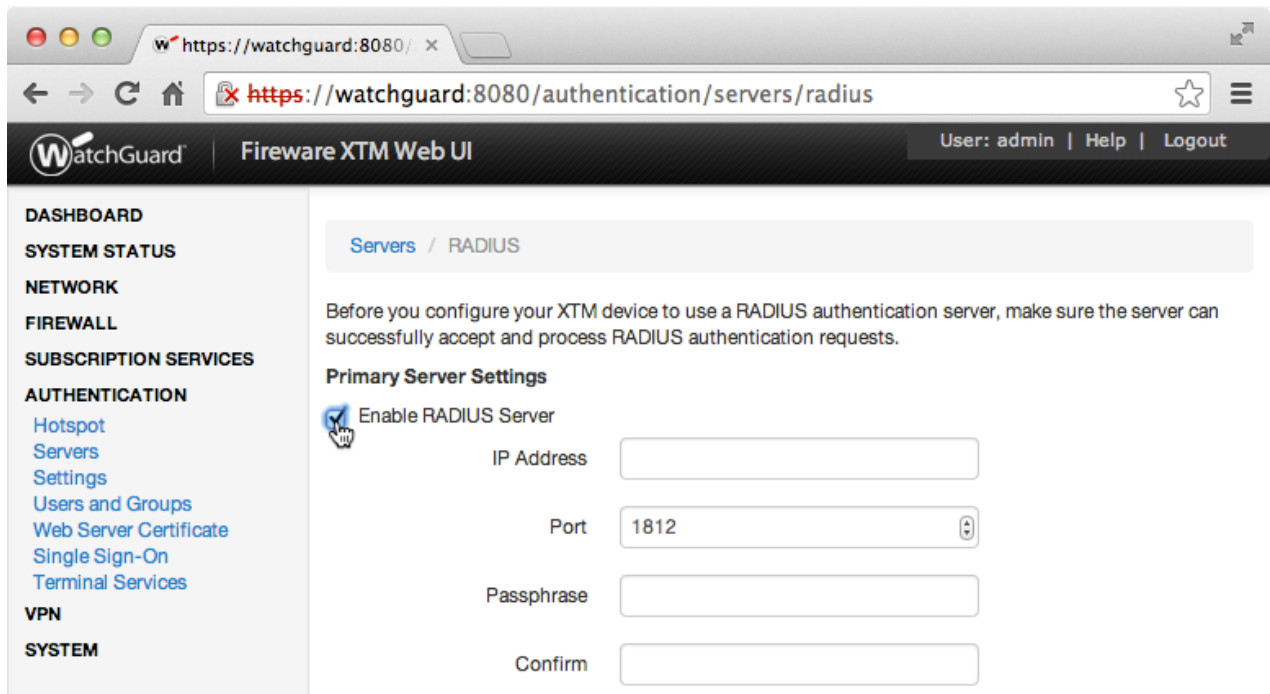
Last 20 Minutes

External Bandwidth

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



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



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

Secondary Server Settings

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 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. 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.

You can also configure the [Secondary Radius Server](#) to provide failover. This prevents the RADIUS Server from dropping authentication requests if it goes offline or receives too many requests.

7. Click **Save**:

Enable Secondary RADIUS Server

IP Address

Port

Passphrase

Confirm

Timeout seconds

Retries

Group Attribute

Dead Time

8. Click **VPN**:

WatchGuard | Fireware XTM Web UI | User: admin | Help | Logout

DASHBOARD
 SYSTEM STATUS
 NETWORK
 FIREWALL
 SUBSCRIPTION SERVICES
 AUTHENTICATION
 Hotspot
 Servers
 Settings
 Users and Groups
 Web Server Certificate
 Single Sign-On
 Terminal Services
VPN
 SYSTEM

Servers

Authentication Servers

Server	Status	
Firebox	0 Users	0 Groups
RADIUS	Primary	10.0.10.130
	Secondary	Disabled
SecurID	Primary	Disabled
	Secondary	Disabled
LDAP	Primary	Disabled
	Secondary	Disabled
Active Directory	0 domains	

9. Under **VPN** click **Mobile VPN with SSL**:

The screenshot shows the WatchGuard Web UI at the URL `https://watchguard:8080/authentication/servers`. The left sidebar contains navigation menus for NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled "Authentication Servers" and displays a table with columns for "Server" and "Status".

Server	Status
Firebox	0 Users 0 Groups
RADIUS	Primary 10.0.10.130
	Secondary Disabled
SecurID	Primary Disabled
	Secondary Disabled
LDAP	Primary Disabled
	Secondary Disabled
Active Directory	0 domains

At the bottom of the page, there is a button labeled "Test Connection for LDAP and Active Directory".

10. Click **Activate Mobile VPN with SSL**:

The screenshot shows the WatchGuard Web UI at the URL `https://watchguard:8080/vpn/ssl`. The left sidebar contains navigation menus for DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled "Mobile VPN with SSL" and contains the following text:

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

Below this, there are three tabs: "General", "Authentication", and "Advanced".

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

Secondary

Networking and IP address pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to

11. Under **Firebox IP Address or Domain Names**

The screenshot shows the WatchGuard Fireware XTM Web UI. The browser address bar displays `https://watchguard:8080/vpn/ssl`. The page title is "Mobile VPN with SSL". A sidebar on the left contains navigation links: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, and VPN (with sub-links for Branch Office VPN, BOVPN Virtual Interfaces, Phase2 Proposals, Mobile VPN with IPSec, Mobile VPN with PPTP, Mobile VPN with SSL, Mobile VPN with L2TP, and Global Settings). The main content area has a header "Mobile VPN with SSL" and a description: "When you activate Mobile VPN with SSL, the 'SSLVPN-Users' group and the 'WatchGuard SSLVPN' policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface." Below this is a checked checkbox "Activate Mobile VPN with SSL". There are three tabs: "General" (selected), "Authentication", and "Advanced". A section titled "Firebox IP Addresses or Domain Names" contains the instruction "Type a firebox IP or domain name for SSL VPN users to connect to." It has two input fields: "Primary" with the value "10.0.10.130" and "Secondary" which is empty. Below this is a section "Networking and IP address pool" with the instruction: "Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to

Property	Explanation	Example
Primary	Primary IP address or domain name Firebox users connect to.	10.0.10.130
Secondary (optional)	Secondary IP address or domain name Firebox users connect to.	10.0.10.131

12. Click **Authentication** tab:

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication Advanced

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

Secondary

Networking and IP address pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to

13. Select **RADIUS**:

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication Advanced

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server.

Sel	Authentication Server
<input type="checkbox"/>	Firebox-DB
<input checked="" type="checkbox"/>	RADIUS (Default)

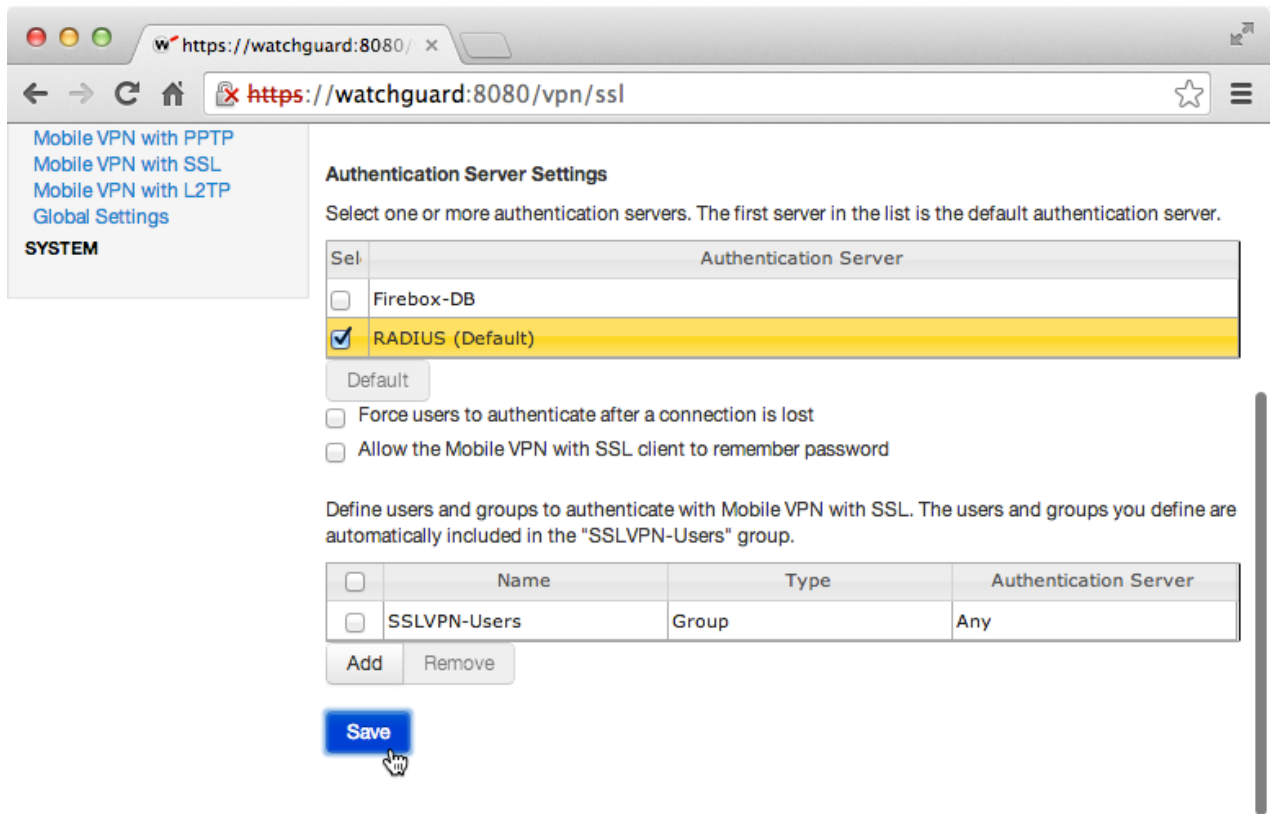
Default

Force users to authenticate after a connection is lost

Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

14. Click **Save**:



You are now ready to test your configuration.

Testing (WatchGuard Configuration)

To test, navigate to your WatchGuard clientless VPN portal or use a WatchGuard client and attempt access.

To test SSL connections, you can use the following online portal:

```
https://[device interface IP  
address]/sslvpn_logon.shtml
```

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:

- Individual users can be added manually in [LoginTC Admin](#)
- Bulk operations in [LoginTC Admin](#)
- Programmatically manage user lifecycle with the [REST API](#)
- One-way user synchronization of users to LoginTC Admin is performed using [LoginTC Sync Tool](#).

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

The screenshot shows the WatchGuard Fireware XTM Web UI interface. The left-hand navigation bar has the **AUTHENTICATION** menu item selected, indicated by a mouse cursor. The main content area displays the **Front Panel** with a **Top Clients** table and a **System** information panel.

Name	Rate	Bytes	Hits
10.0.88.100	531 Kbps	21 MB	21
10.0.88.104	211 Kbps	9 MB	14
10.0.88.102	29 Kbps	9 MB	13

System

Name	XTM_2_Series-W
Model	XTM26-W
Version	11.9.5.B470931
Serial Number	70A70CDC3D640
System Time	14:42 US/Eastern
System Date	2015-06-17
Uptime	2 days 01:55

2. Click **Servers**

The screenshot shows the WatchGuard Fireware XTM Web UI interface. The left-hand navigation bar has the **AUTHENTICATION** menu item selected, and the **Servers** sub-menu item is highlighted with a mouse cursor. The main content area displays the **Front Panel** with a **Top Clients** table, a **Top Destinations** table, and a **System** information panel.

Name	Rate	Bytes	Hits
10.0.88.100	151 Kbps	3 MB	22
10.0.88.104	105 Kbps	8 MB	118
10.0.88.102	28 Kbps	9 MB	14

Top Destinations

Name	Rate	Bytes	Hits
184.150.152.14	126 Kbps	2 MB	1
74.125.29.101	20 Kbps	646 KB	1
136.146.210.32	19 Kbps	177 KB	2
184.150.152.18	18 Kbps	137 KB	2

System

Name	XTM_2_Series-W
Model	XTM26-W
Version	11.9.5.B470931
Serial Number	70A70CDC3D640
System Time	14:43 US/Eastern
System Date	2015-06-17
Uptime	2 days 01:56
Log Server	Disabled

Reboot

Last 20 Minutes

3. Select **RADIUS**

WatchGuard | Fireware XTM Web UI | User: admin | Help | Logout

DASHBOARD
SYSTEM STATUS
NETWORK
FIREWALL
SUBSCRIPTION SERVICES
AUTHENTICATION
Hotspot
Servers
Settings
Users and Groups
Web Server Certificate
Single Sign-On
Terminal Services
Authentication Portal
VPN
SYSTEM

Servers

Authentication Servers

Server	Status	
Firebox	0 Users	2 Groups
<u>RADIUS</u>	Primary	10.0.10.83
	Secondary	Disabled
SecurID	Primary	Disabled
	Secondary	Disabled
LDAP	Primary	Disabled
	Secondary	Disabled

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

Dead Time Hours

Secondary Server Settings

Enable Secondary RADIUS Server

IP Address

Port

Passphrase

Confirm

Timeout seconds

Retries

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

Secondary Server Settings

Enable Secondary RADIUS Server

IP Address

Port

Passphrase

Confirm

Timeout seconds

Retries

Group Attribute

Dead Time

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. At least 60s.	120
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**

Retries

Group Attribute

Dead Time

LoginTC RADIUS Connector Has No Network Connection

1. First ensure that your LoginTC RADIUS Connector is configured to have a virtual network adapter on `eth0`
2. Ensure that the virtual network adapter MAC address matches the one in the file `/etc/sysconfig/network-scripts/ifcfg-eth0`
3. Restart the networking service:

```
service network  
restart
```

4. If you notice the error that `eth0` is not enabled, then check driver messages for more information:

```
dmesg | grep  
eth
```

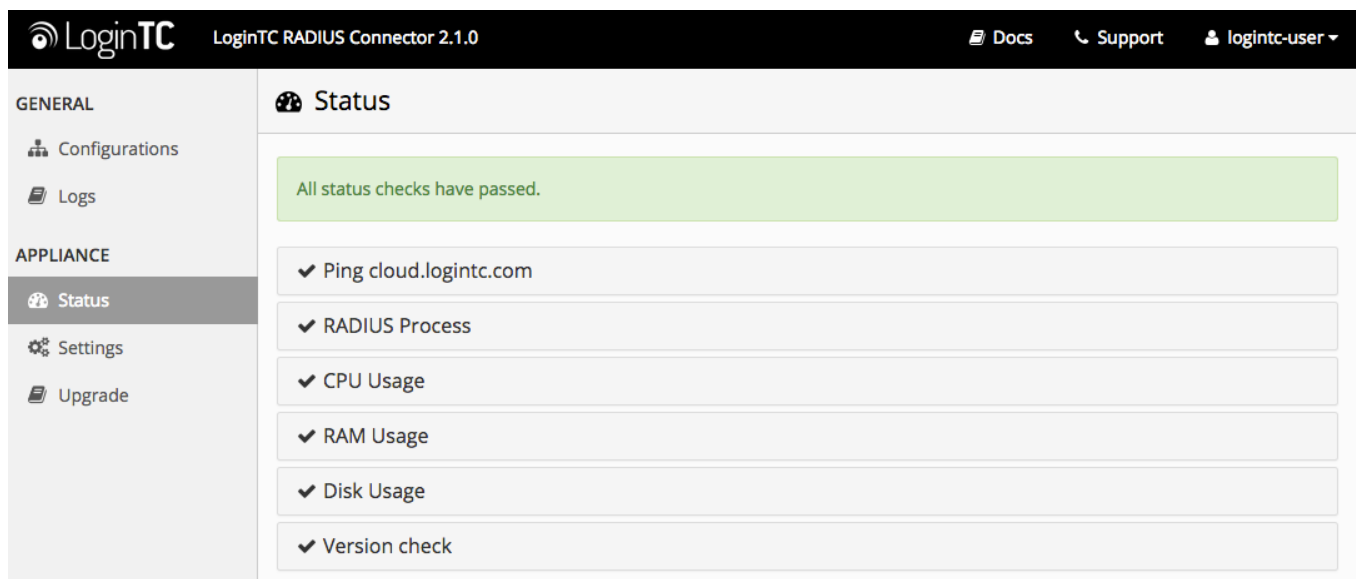
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

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

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


Not Authenticating

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



The screenshot shows the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the version "LoginTC RADIUS Connector 2.1.0", and links for "Docs", "Support", and a user profile "logintc-user". The left sidebar has a "GENERAL" section with "Configurations" and "Logs", and an "APPLIANCE" section with "Status", "Settings", and "Upgrade". The main content area is titled "Status" and displays a green message: "All status checks have passed." Below this, there are six 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**:

 LoginTC RADIUS Connector 2.1.0

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

GENERAL

- Configurations
- Logs**

APPLIANCE

- Status
- Settings
- Upgrade

Logs

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

```

2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms
2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms
2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms
2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms
2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms
2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms
2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms
2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms
    
```

Displaying last 1000 lines, refreshes automatically every 1 second.

[Download](#)

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:

 Fireware XTM Web UI
 User: admin | [Help](#) | [Logout](#)

DASHBOARD

- SYSTEM STATUS**
- NETWORK
- FIREWALL
- SUBSCRIPTION SERVICES
- AUTHENTICATION
- VPN
- SYSTEM

Front Panel

Top Clients			
Name	Rate	Bytes	Hits
10.0.88.104	166 Kbps	11 MB	64
10.0.88.100	107 Kbps	720 KB	37
10.0.88.102	73 Kbps	9 MB	17

System	
Name	XTM_2_Series-W
Model	XTM26-W
Version	11.9.5.B470931
Serial Number	70A70CDC3D640
System Time	14:52 US/Eastern
System Date	2015-06-17
Uptime	2 days 02:05
Log Server	Disabled

Click on **Traffic Monitor**:

WatchGuard | Fireware XTM Web UI User: admin | Help | Logout

DASHBOARD

- Front Panel
- Subscription Services
- FireWatch
- Interfaces
- Traffic Monitor
- Gateway Wireless Controller

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

Front Panel ↻

Top Clients

Name	Rate ↓	Bytes	Hits
10.0.88.104	138 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	11 MB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	57 <input type="checkbox"/>
10.0.88.100	61 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	873 KB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	36 <input type="checkbox"/>
10.0.88.102	35 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	10 MB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	14 <input type="checkbox"/>

Top Destinations

Name	Rate ↓	Bytes	Hits
184.150.152.15	65 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	1 MB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	3 <input type="checkbox"/>
74.125.22.139	53 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	2 MB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	1 <input type="checkbox"/>
10.0.10.164	14 Kbps <div style="width: 100%; height: 10px; background: linear-gradient(to right, orange, red);"></div>	11 MB <div style="width: 100%; height: 10px; background: linear-gradient(to right, green, blue);"></div>	2 <input type="checkbox"/>

System

Name **XTM_2_Series-W**

Model **XTM26-W**

Version **11.9.5.B470931**

Serial Number **70A70CDC3D640**

System Time **14:53 US/Eastern**

System Date **2015-06-17**

Uptime **2 days 02:06**

Log Server **Disabled**

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

WatchGuard | Fireware XTM Web UI User: admin | Help | Logout

DASHBOARD

- Front Panel
- Subscription Services
- FireWatch
- Interfaces
- Traffic Monitor
- Gateway Wireless Controller

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

Traffic Monitor ⏸

📅
🌐
👤
📊
🔍

```

2015-06-17 15:03:23 sessiond sessiond: sessiond WGAPI call
2015-06-17 15:03:23 sessiond sessiond: wgapi: rcved cmd=1 '/toSessiond/updateActivity' fromIPC=-61236
2015-06-17 15:03:23 sessiond sessiond: get into sess_prcc_status(): xpath=/toSessiond/updateActivity
2015-06-17 15:03:23 sessiond OK! sess update oK, sessId=28
2015-06-17 15:03:26 Deny 10.0.10.176 10.0.10.255 netbios-ns/udp 137 137 0-External Firebox Denied 78
2015-06-17 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff:62 IEEE 802.11: authenticated
2015-06-17 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff:62 IEEE 802.11: associated (aid 3)
2015-06-17 15:03:37 Deny 10.0.88.100 255.255.255.255 17500/udp 17500 17500 1-WG-Wireless-Access-
2015-06-17 15:03:39 Deny 10.0.20.30 10.0.10.1 dns/udp 58082 53 0-External Firebox Denied 51 63 (Unha
2015-06-17 15:03:39 Deny 10.0.20.30 10.0.10.1 dns/udp 51650 53 0-External Firebox Denied 65 63 (Unha
2015-06-17 15:03:43iked ***** RECV message on fd_server(7) *****
2015-06-17 15:03:43iked recv CMD XPATH(/ping), need to process it
2015-06-17 15:03:43 sessiond sessiond: sessiond WGAPI call
2015-06-17 15:03:43 sessiond sessiond: wgapi: rcved cmd=7 '/ping' fromIPC=784335663 serial=70A70CD
2015-06-17 15:03:46 Deny 10.0.10.176 10.0.10.8 2054/udp 54312 2054 0-External Firebox Denied 56 128

```

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:

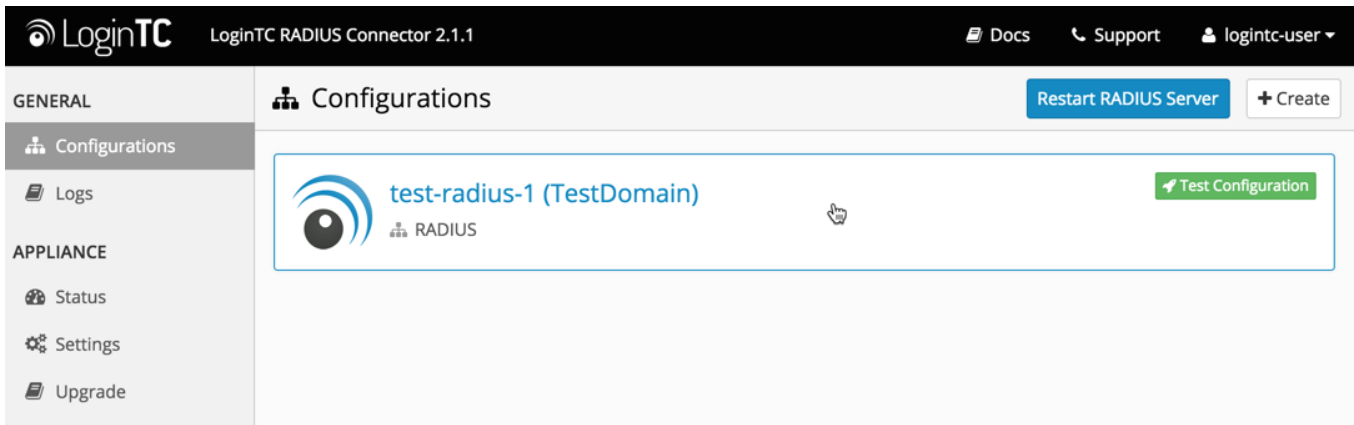
```

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

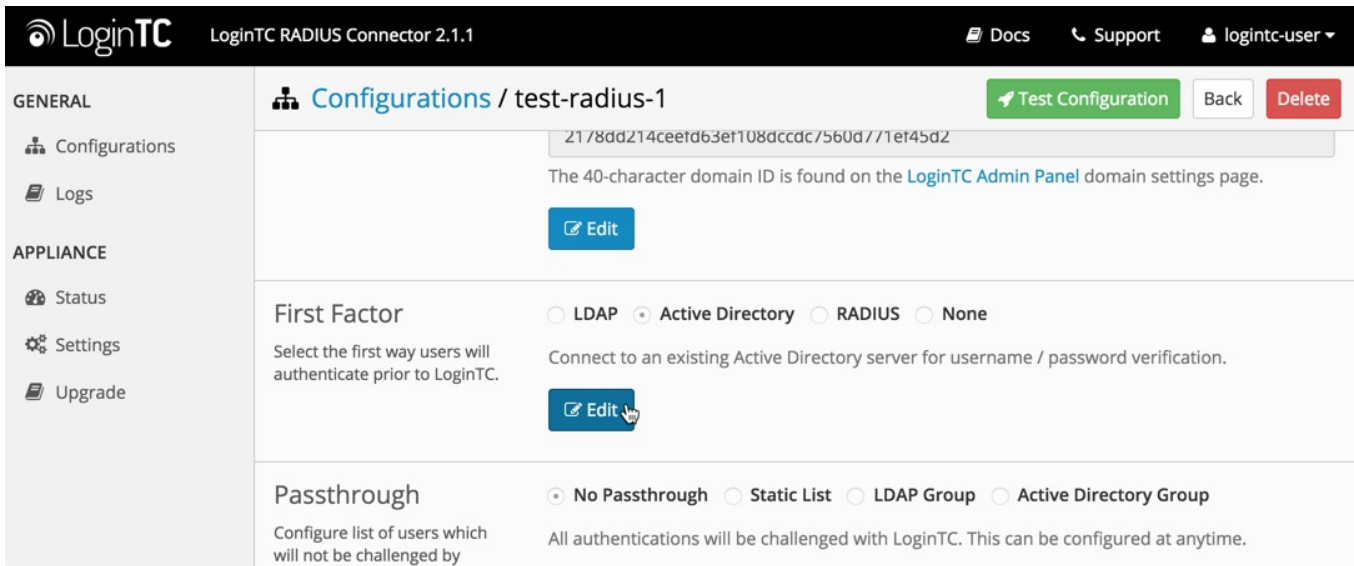
```

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:

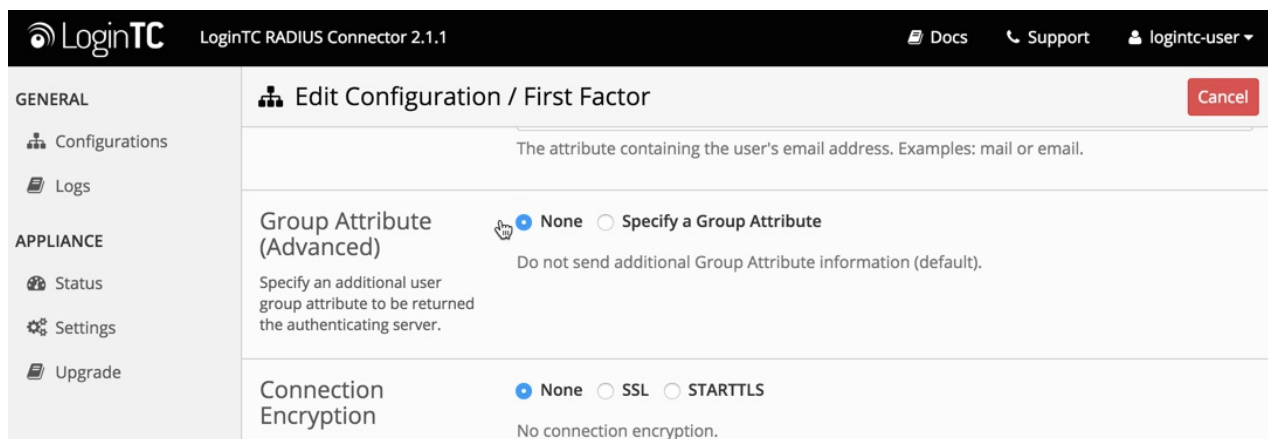


Click the **Edit Button** in the **First Factor** section:

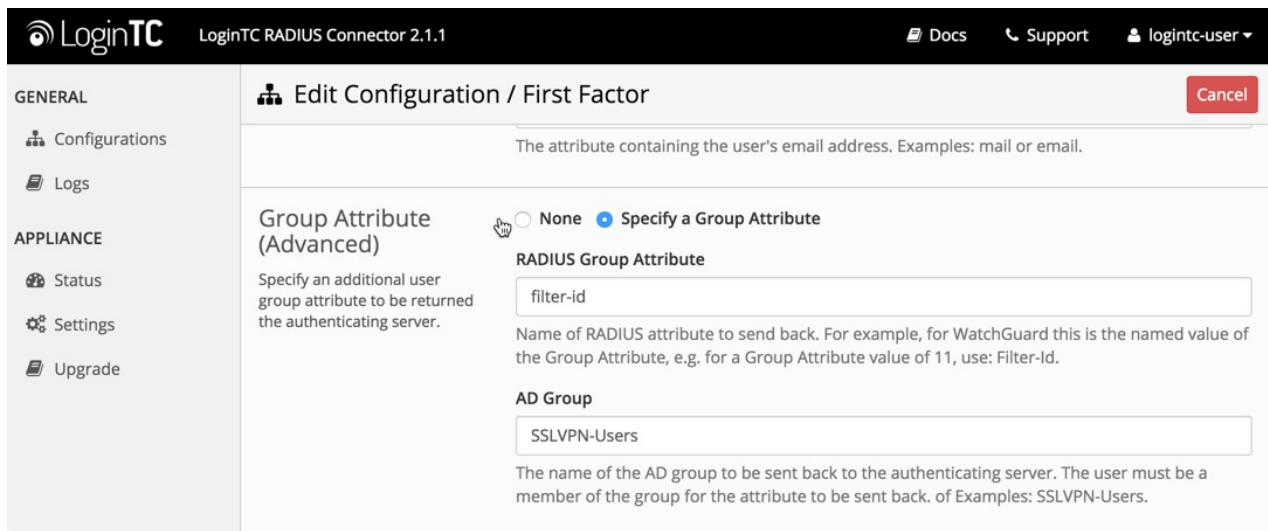


Scroll down to the to the **Group Attribute** section:

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.

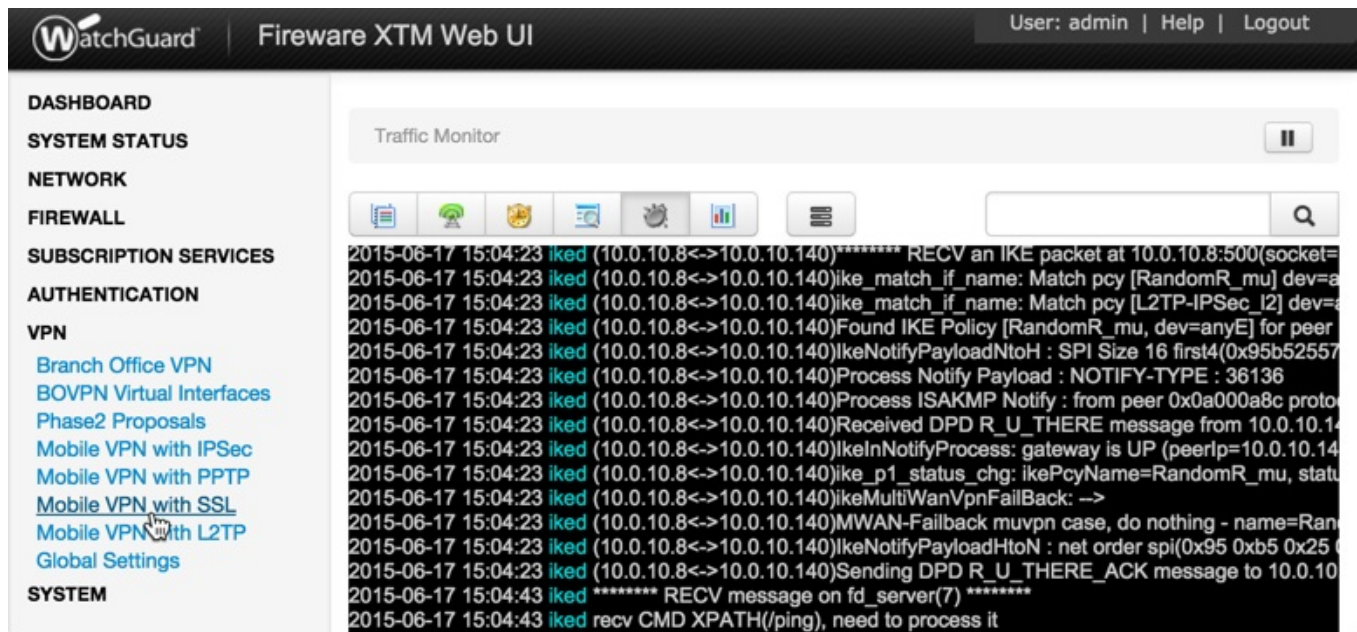


If you find a log message similar to this:

```
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:

WatchGuard | Fireware XTM Web UI User: admin | Help | Logout

DASHBOARD
SYSTEM STATUS
NETWORK
FIREWALL
SUBSCRIPTION SERVICES
AUTHENTICATION
VPN
 Branch Office VPN
 BOVPN Virtual Interfaces
 Phase2 Proposals
 Mobile VPN with IPSec
 Mobile VPN with PPTP
 Mobile VPN with SSL
 Mobile VPN with L2TP
 Global Settings
SYSTEM

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General **Authentication** Advanced

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

Secondary

Networking and IP address pool

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:

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

<input type="checkbox"/>	Name	Type	Authentication Server
<input type="checkbox"/>	SSLVPN-Users	Group	Any

Add Remove

Save

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

Mobile VPN with L2TP
 Global Settings
 SYSTEM

RADIUS (Default)

Add User or Group ✕

Type Group
 User

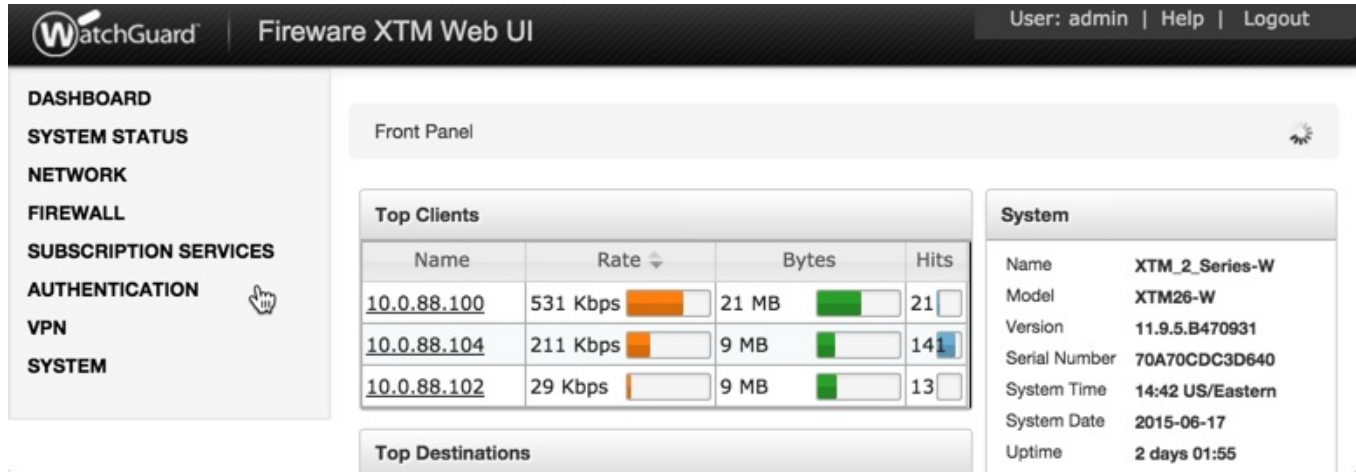
Name

Authentication Server

OK Cancel

Authentication Requests 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 60 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**

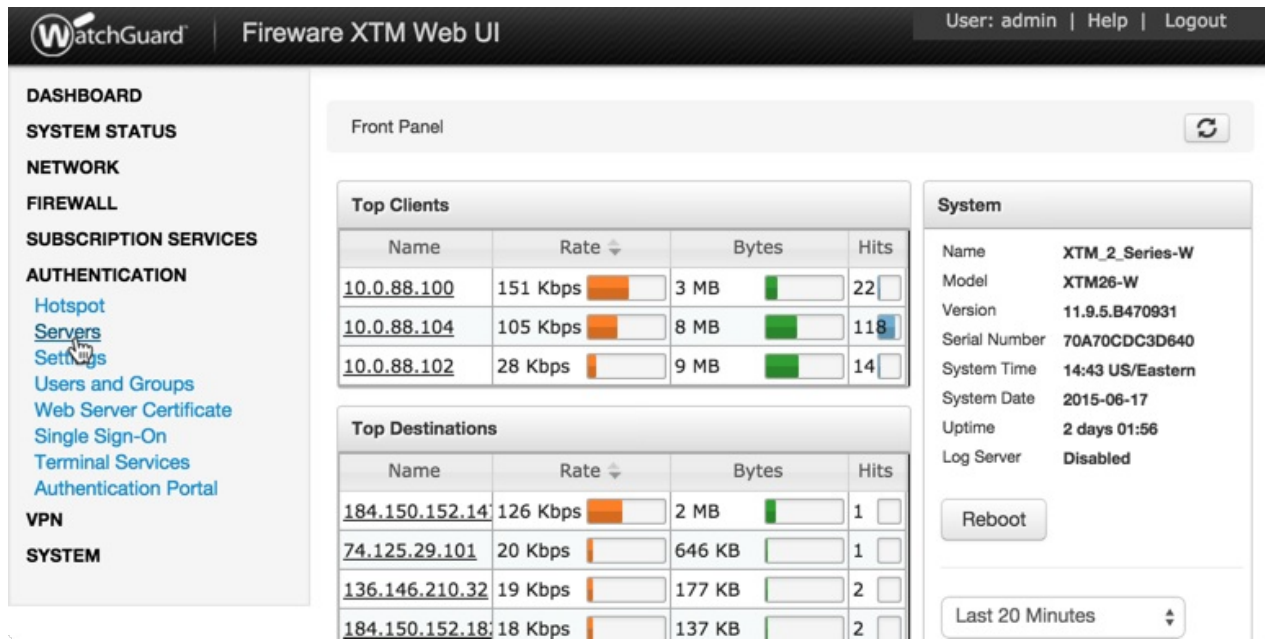


The screenshot shows the WatchGuard Fireware XTM Web UI interface. The left-hand navigation bar has the **AUTHENTICATION** menu item selected, indicated by a mouse cursor. The main content area displays the **Front Panel** with the following data:

Top Clients			
Name	Rate	Bytes	Hits
10.0.88.100	531 Kbps	21 MB	21
10.0.88.104	211 Kbps	9 MB	141
10.0.88.102	29 Kbps	9 MB	13

System	
Name	XTM_2_Series-W
Model	XTM26-W
Version	11.9.5.B470931
Serial Number	70A70CDC3D640
System Time	14:42 US/Eastern
System Date	2015-06-17
Uptime	2 days 01:55

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



The screenshot shows the WatchGuard Fireware XTM Web UI interface with the **Servers** menu item selected under the **AUTHENTICATION** category. The main content area displays the **Front Panel** with the following data:

Top Clients			
Name	Rate	Bytes	Hits
10.0.88.100	151 Kbps	3 MB	22
10.0.88.104	105 Kbps	8 MB	118
10.0.88.102	28 Kbps	9 MB	14

Top Destinations			
Name	Rate	Bytes	Hits
184.150.152.14	126 Kbps	2 MB	1
74.125.29.101	20 Kbps	646 KB	1
136.146.210.32	19 Kbps	177 KB	2
184.150.152.18	18 Kbps	137 KB	2

System	
Name	XTM_2_Series-W
Model	XTM26-W
Version	11.9.5.B470931
Serial Number	70A70CDC3D640
System Time	14:43 US/Eastern
System Date	2015-06-17
Uptime	2 days 01:56
Log Server	Disabled

Reboot

Last 20 Minutes

2. Click **RADIUS**

Servers

Authentication Servers

Server	Status	Users	Groups
Firebox		0 Users	2 Groups
<u>RADIUS</u>	Primary		10.0.10.83
	Secondary		Disabled
SecurID	Primary		Disabled
	Secondary		Disabled
LDAP	Primary		Disabled
	Secondary		Disabled

3. Check the **Timeout** attribute field. It should be at least 60 seconds.

Servers / RADIUS

Before you configure your XTM device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.

Primary Server Settings

Enable RADIUS Server

IP Address: 10.0.10.83

Port: 1812

Passphrase:

Confirm:

Timeout: 120 seconds
Range: 1-120 Default: 5

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`
`curl -O https://www.logintc.com/downloads/logintc-radius-connector-2.1.1-upgrade.tar.gz`
3. `(SHA-1: 8b3709611a8759911283cce9fce9efe4e628dfdb)`
`tar -xf logintc-radius-connector-2.1.1-upgrade.tar.gz`
4. `upgrade.tar.gz`

```
sudo sh logintc-radius-connector-2.1.1-  
5. upgrade/upgrade.sh
```