

# Two factor authentication for WatchGuard XTM and Firebox

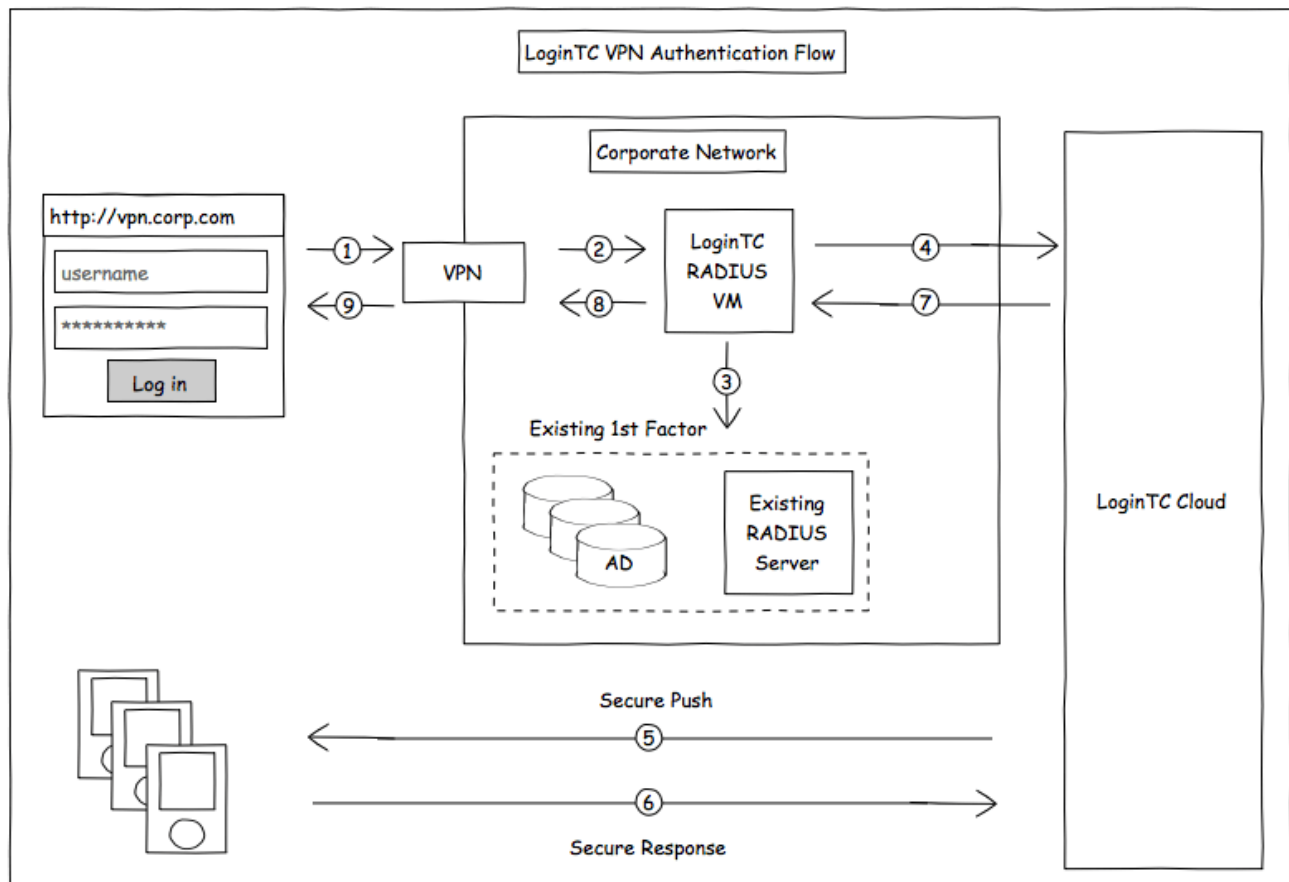
[loginfc.com/docs/connectors/watchguard.html](http://loginfc.com/docs/connectors/watchguard.html)

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 instructions using direct authentication then you may be interested in: [Two factor authentication for WatchGuard](#).

## User Experience

After entering the username and password into the Mobile VPN client, the user is presented with an Authentication Message. The user may enter '1' to receive a push notification to their device to approve or enter a valid One-Time Password (OTP). This flow works the same for clientless access.

## Architecture



## 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 are supported. For example, WatchGuard Mobile VPN with SSL.

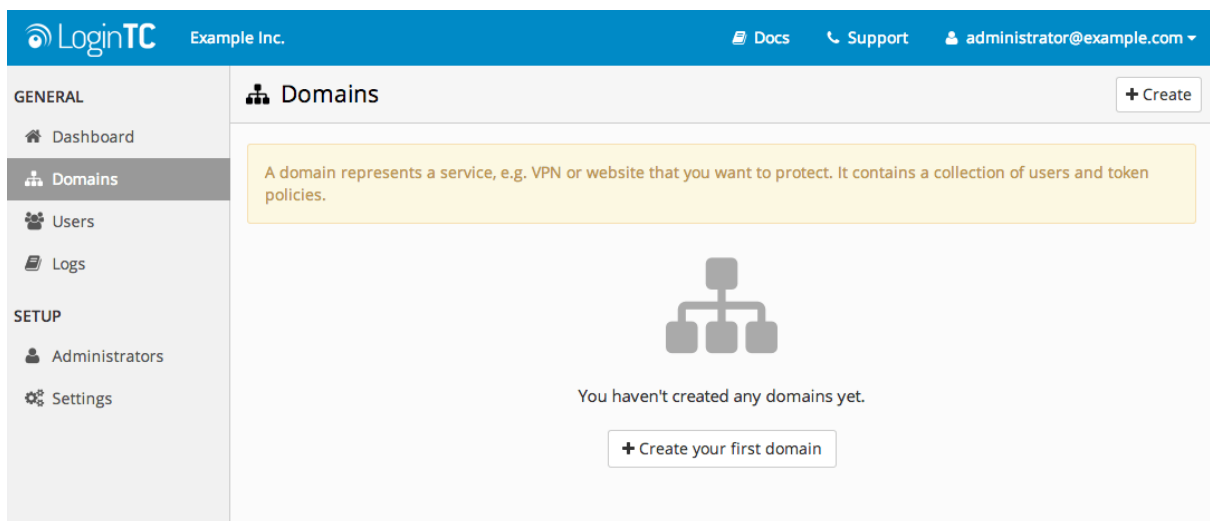
## Prerequisites

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:

Example Inc.

Docs

Support

administrator@example.com

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 6.8 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) |

3/32

| 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

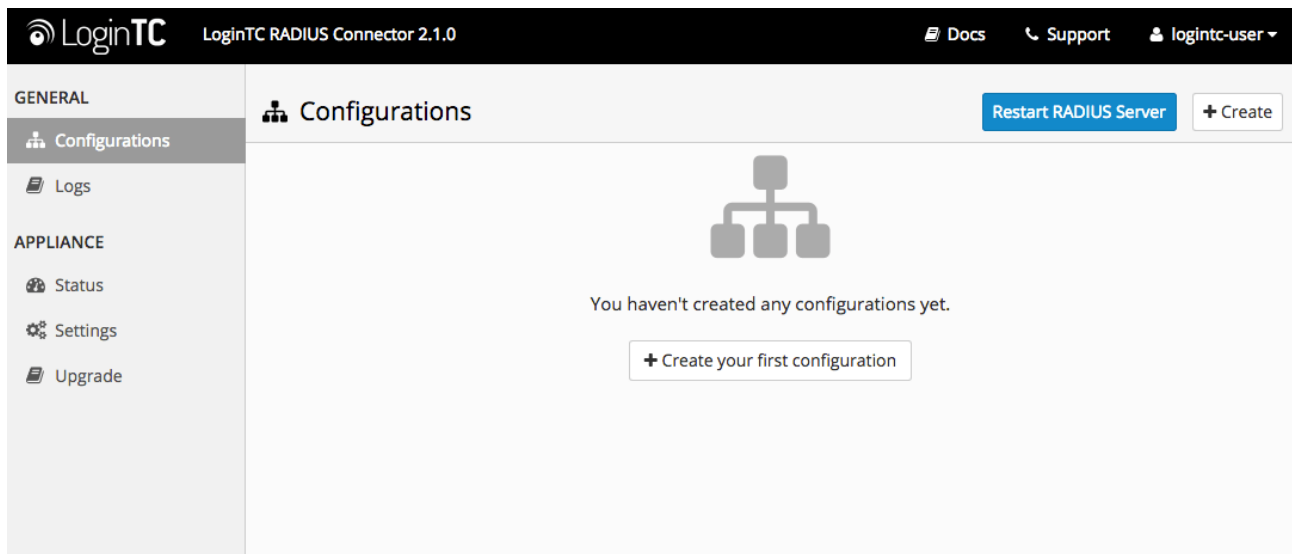
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

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

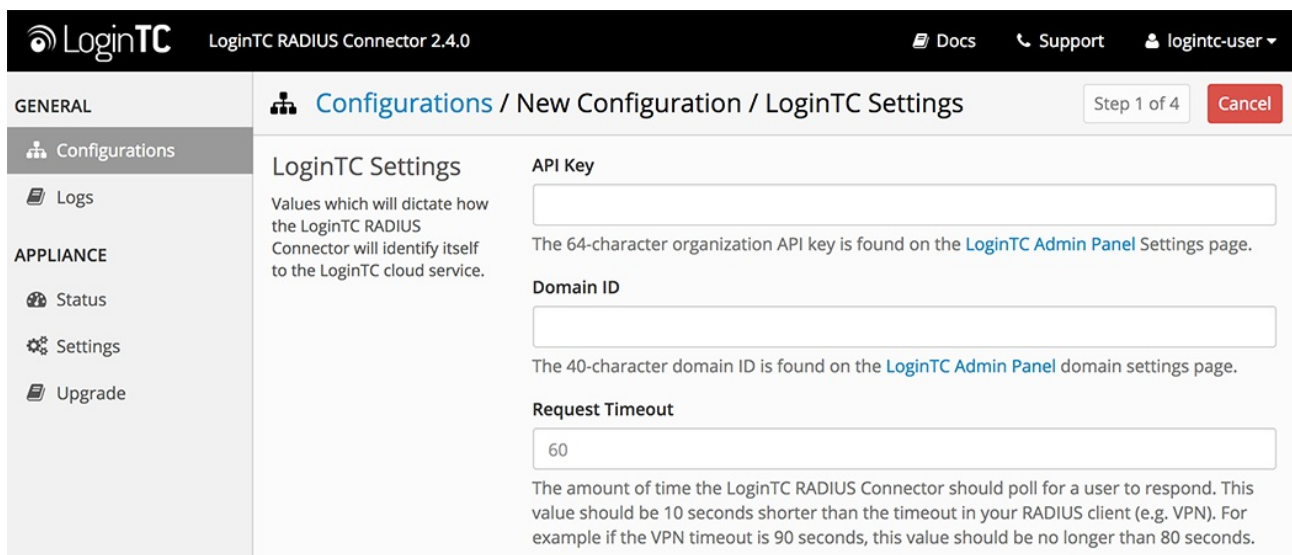
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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**:

The screenshot shows the 'New Configuration / LoginTC Settings' page in the LoginTC RADIUS Connector 2.1.0 interface. The page is divided into a left sidebar with 'GENERAL' and 'APPLIANCE' sections, and a main content area. The 'GENERAL' section is active, showing 'Configurations' and 'Logs' options. The 'APPLIANCE' section shows 'Status', 'Settings', and 'Upgrade' options. The main content area is titled 'New Configuration / LoginTC Settings' and includes a 'Step 1 of 4' indicator and a 'Cancel' button. Below the title, there is a 'LoginTC Settings' section with a description: 'Values which will dictate how the LoginTC RADIUS Connector will identify itself to the LoginTC cloud service.' This section contains two input fields: 'API Key' with the value 'vZkDw7l6Z3tApwZjXERseKdR0s5RNNqjMxXIwvxPWWjOa9ojXi9b5tdvPyFsqzwj' and 'Domain ID' with the value '9120580e94f134cb7c9f27cd1e43dbc82980e152'. Below the input fields, there is a note for each field explaining where to find the values. At the bottom of the main content area, there are 'Test' and 'Next' buttons. A green message box at the bottom of the page states '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

New Configuration / First Factor

Step 2 of 4

Cancel

First Factor

☒ LDAP
☐ Active Directory
☐ RADIUS
☐ None

Select the first way users will authenticate prior to LoginTC.

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

LDAP Server Details

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 RADIUS Connector 2.1.0

Docs
Support
logintc-user

GENERAL

Configurations
Logs

APPLIANCE

Status
Settings
Upgrade

New Configuration / First Factor

Step 2 of 4

Cancel

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)

389

Port if Active Directory server uses non-standard port.

Bind Details

☒ Bind with credentials
☐ Anonymous

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                |

7/32

| Property                                    | Explanation   | Examples   |
|---|---|--|
| <code>attr_username</code>                  | The attribute containing the user's username  | <code>sAMAccountName</code> or <code>uid</code>                          |
| <code>attr_name</code>                      | The attribute containing the user's real name   | <code>displayName</code> or <code>cn</code>                              |
| <code>attr_email</code>                     | The attribute containing the user's email address   | <code>mail</code> or <code>email</code>                                  |
| <b>Group Attribute</b><br>(optional)        | Specify an additional user group attribute to be returned the authenticating server.  | <code>SSLVPN-Users</code>  |
| <b>RADIUS Group Attribute</b><br>(optional) | Name of RADIUS attribute to send back   | <code>Filter-Id</code>   |
| <b>LDAP Group / AD Group</b><br>(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. | <code>SSLVPN-Users</code> or <code>Administrators,Sales,Engineers</code> |
| <b>encryption</b><br>(optional)             | Encryption mechanism  | <code>ssl</code> or <code>startTLS</code>                                |
| <b>cacert</b><br>(optional)                 | CA certificate file (PEM format)  | <code>/opt/logintc/cacert.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.

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**New Configuration / First Factor** Step 2 of 4 **Cancel**

**Group Attribute (Advanced)**

Specify an additional user group attribute to be returned the authenticating server.

☐ None ☒ Specify a Group Attribute

**RADIUS Group Attribute**

Filter-Id

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.

**LDAP Group**

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**:

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**New Configuration / First Factor** Step 2 of 4 **Cancel**

**First Factor**

Select the first way users will authenticate prior to LoginTC.

☐ LDAP ☐ Active Directory ☒ RADIUS ☐ None

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

**RADIUS Server Details**

The RADIUS host and secret.

**Host**

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

**Port (optional)**

1812

Port if the RADIUS server uses non-standard port.

**Secret**

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.

The screenshot shows the LoginTC web interface for configuring a new passthrough. The top navigation bar includes the LoginTC logo, 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 'New Configuration / Passthrough' and shows 'Step 3 of 4'. Under the 'Passthrough' heading, there are four radio button options: 'No Passthrough' (which is selected), 'Static List', 'LDAP Group', and 'Active Directory Group'. Below these options, a text box explains: '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 located at the bottom of the configuration area.

### Static List

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

LoginTC RADIUS Connector 2.1.0

Docs
Support
logintc-user

GENERAL

Configurations
Logs

APPLIANCE

Status
Settings
Upgrade

New Configuration / Passthrough

Step 3 of 4

Cancel

Passthrough

☐ No Passthrough
☒ Static List
☐ LDAP Group
☐ Active Directory Group

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

Static List

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

LoginTC challenge 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.

LoginTC RADIUS Connector 2.1.0

Docs
Support
logintc-user

GENERAL

Configurations
Logs

APPLIANCE

Status
Settings
Upgrade

New Configuration / Passthrough

Step 3 of 4

Cancel

Passthrough

☐ No Passthrough
☐ Static List
☐ LDAP Group
☒ Active Directory Group

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

Auth Groups

Only users which are members of one or more of the specified groups will be challenged with LoginTC. All other users will be challenged with configured first factor only.

LoginTC challenge Auth Groups

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

AD Server Details

The Active Directory host and port information.

Host

Configuration values:

| Property                      | Explanation  | Examples                         |
|-------------------------------|--|----------------------------------|
| LoginTC challenge auth groups | Comma separated list of groups for which users will be challenged with LoginTC | SSLVPN-Users or two-factor-users |

11/32

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

## Configuration Simplified

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

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

## Client and Encryption

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

LoginTC RADIUS Connector 2.1.0

Docs
Support
logintc-user

GENERAL

Configurations
Logs

APPLIANCE

Status
Settings
Upgrade

New Configuration / Client and Encryption

Step 4 of 4

Cancel

Client Settings

Settings for your RADIUS client (e.g. a RADIUS-speaking VPN) to connect to the LoginTC RADIUS Connector.

Name

A unique identifier of your RADIUS client. Use only alphanumeric characters and hyphens. This will also be used for the name of the configuration file. Example: corp-vpn-1 will be saved on disk as corp-vpn-1.cfg.

IP Address

The IP address of your RADIUS client.

Secret

The secret shared between your RADIUS client and the LoginTC RADIUS Connector.

Encryption

Determine whether to store passwords and API keys encrypted or in the clear.

☒ Encrypt all passwords and API keys

It is strongly recommended to encrypt all sensitive fields.

Client configuration values:

| 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 **Challenge**

LoginTC RADIUS Connector 2.5.1

Docs
Support
logintc-user

GENERAL

Configurations
Logs

APPLIANCE

Status
Settings

Configurations / New Configuration / Client and Encryption

Step 4 of 4

Cancel

Authentication Mode

How the LoginTC RADIUS Connector will perform the second factor.

☐ Direct
☐ Iframe
☒ Challenge

The user will be prompted on how they wish to proceed with second-factor authentication (e.g. LoginTC Push, OTP, bypass code). Your RADIUS client must support RADIUS challenges to use this. Challenging the user will often result in a better user experience.

Challenge Message

Press 1 to authenticate with the LoginTC app or enter an OTP or bypass code.

The message that will appear to the user for the challenge. Note that the user must enter 1 for a LoginTC Push, or must enter an OTP or bypass code.

Encryption

Determine whether to store passwords and API keys encrypted or in the clear.

☒ Encrypt all passwords and API keys

It is strongly recommended to encrypt all sensitive fields.

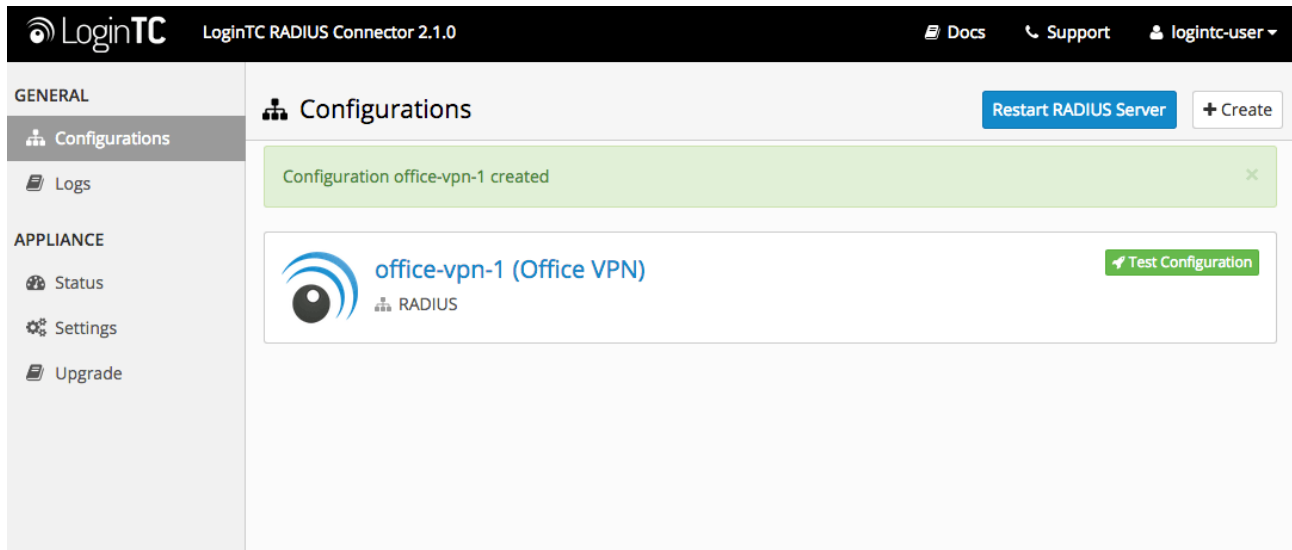
The user will be prompted on how they wish to proceed with second-factor authentication (e.g. LoginTC Push, OTP, bypass code). Your RADIUS client must support RADIUS challenges to use this. Challenging the user will often result in a better user experience. See [User Experience](#) for more information.

## Data Encryption

13/32

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

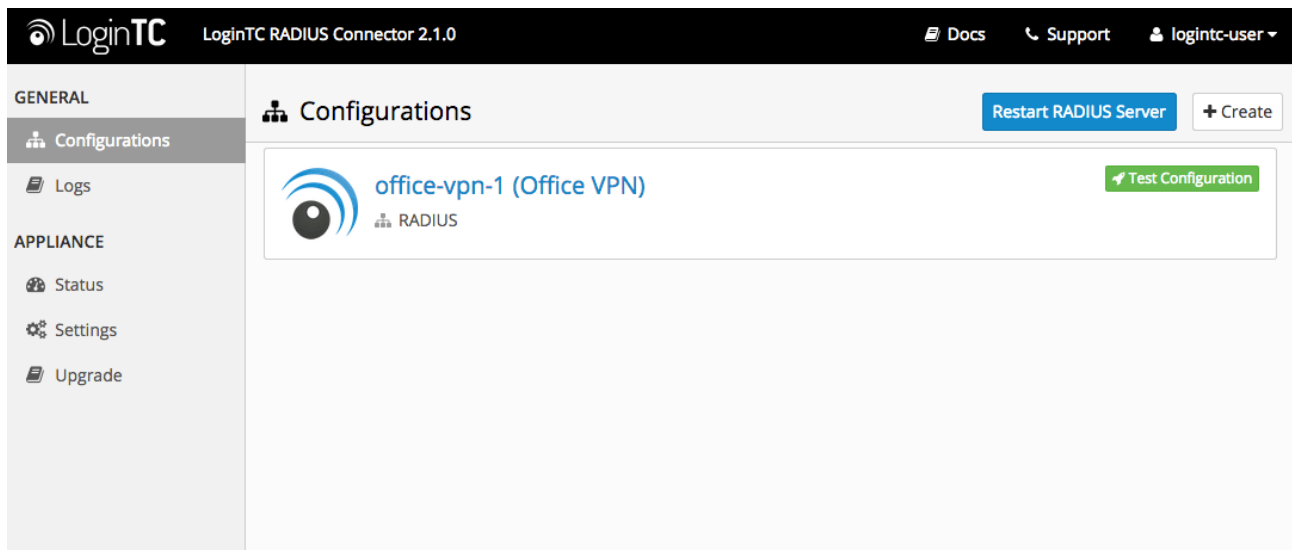
Click **Test** to validate the values and then click **Save**.



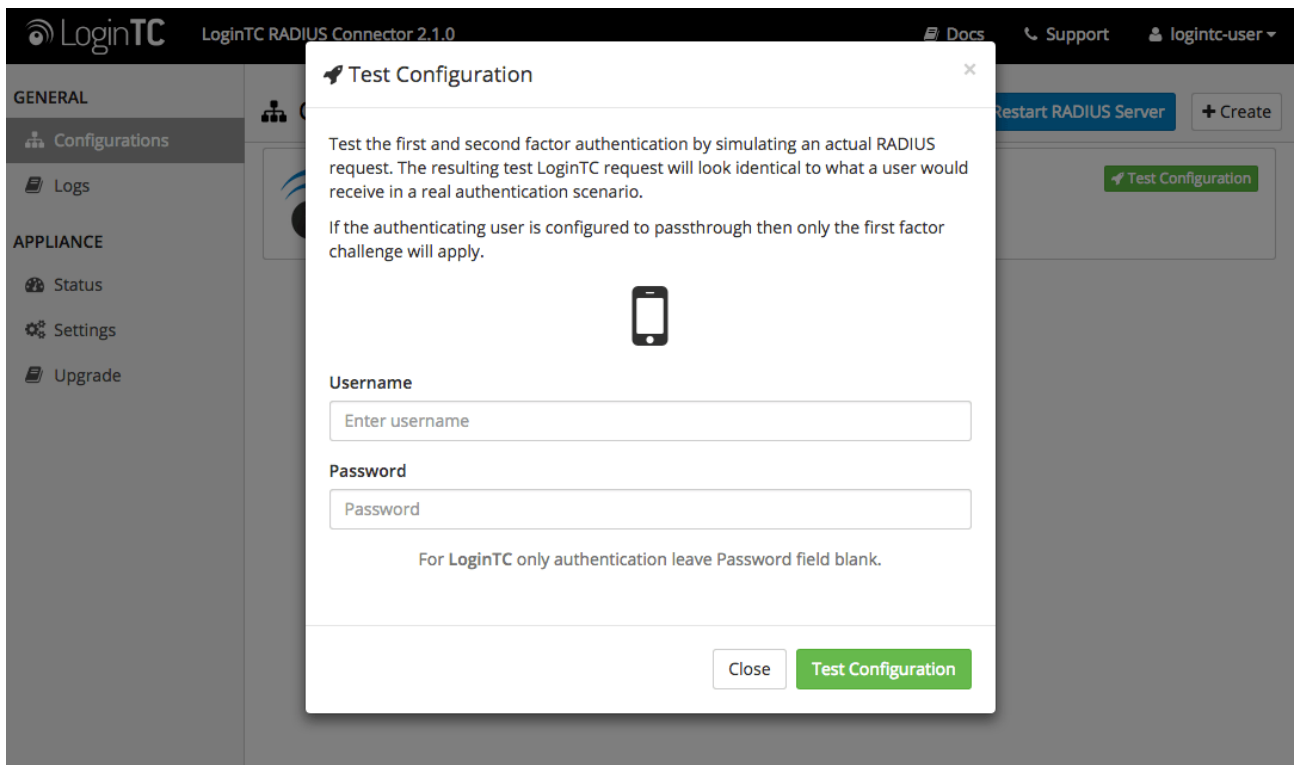
## Testing (Connector)

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:

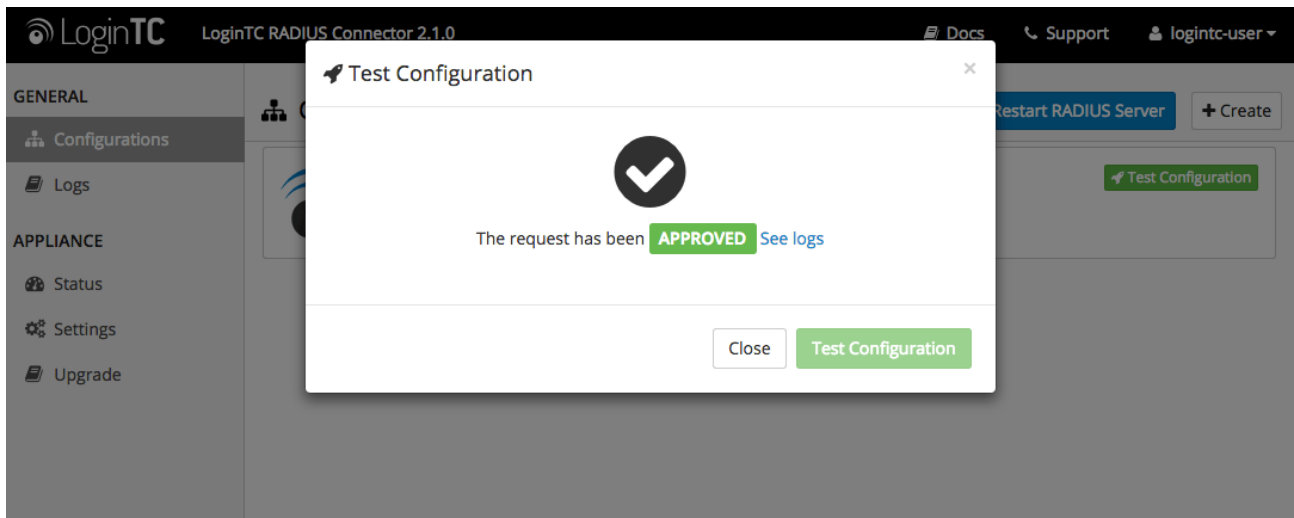
When you have loaded a token for your new user and domain, navigate to your appliance **web interface URL**:



Click **Test Configuration**:

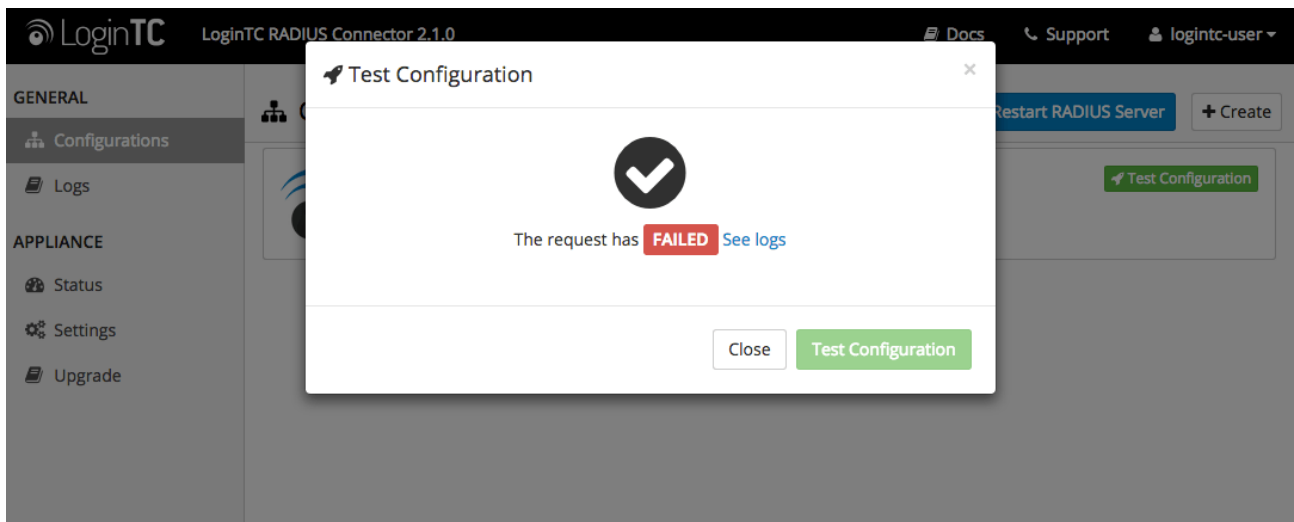


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

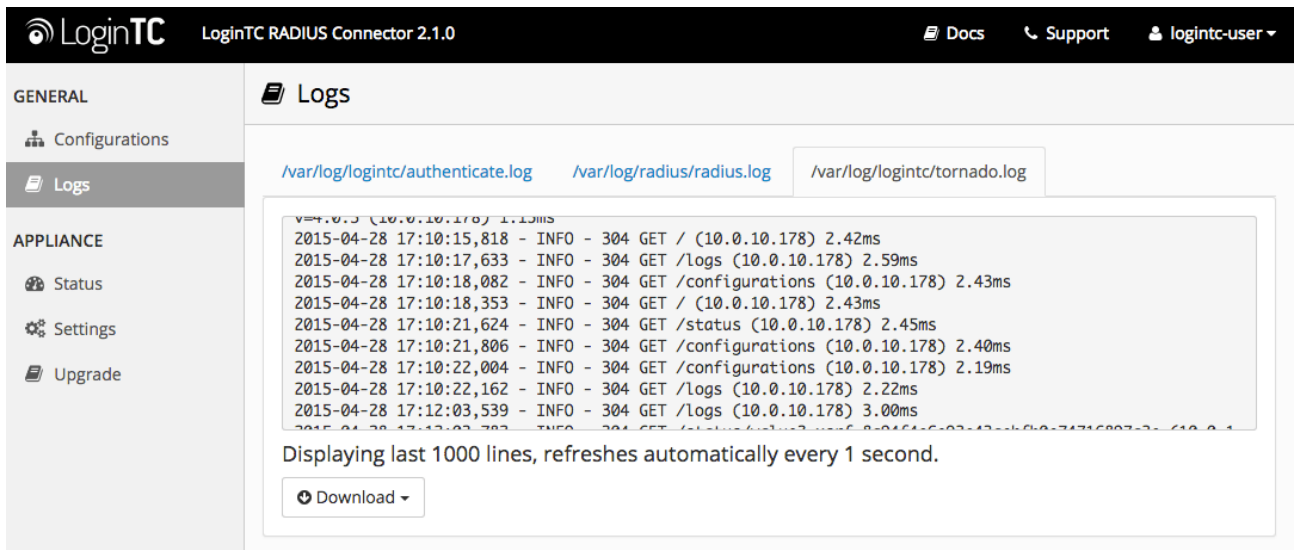


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



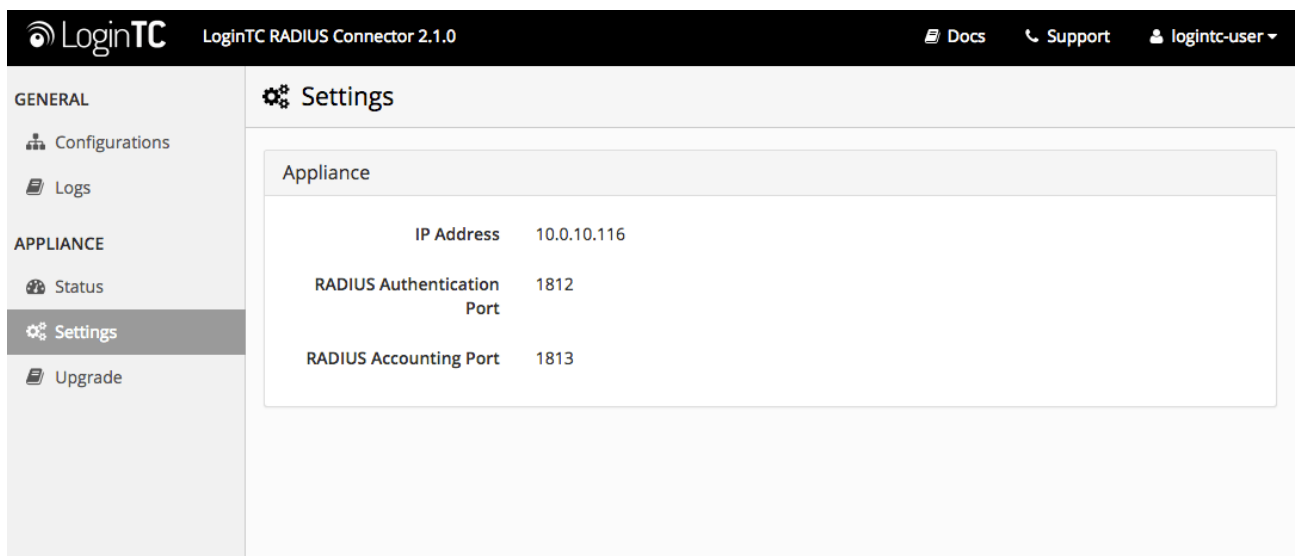
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:



## WatchGuard - Quick Config Guide

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

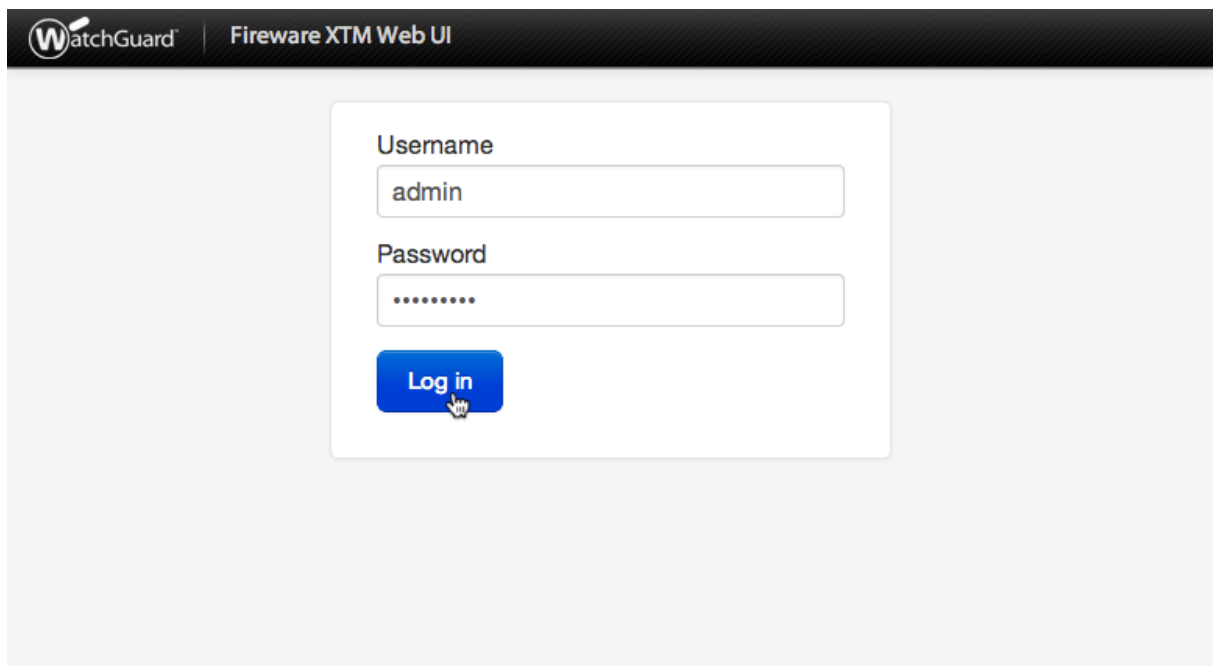
For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:



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

## Mobile VPN with SSL

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



2. Click **Authentication**:

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 |
|-------------|----------|--------|------|
| 10.0.1.5    | 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 V1C5000000000  
 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**:

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**  
[Hotspot](#)  
[Servers](#)  
[Settings](#)  
[Users and Groups](#)  
[Web Server Certificate](#)  
[Single Sign-On](#)  
[Terminal Services](#)

**VPN**

**SYSTEM**

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    |

**Top Policies**

| Name | Rate | Bytes | Hits |
|------|------|-------|------|
|------|------|-------|------|

**System**

Name XTMv  
 Model XTMv  
 Version 11.8.B432340  
 Serial Number V1C5000000000  
 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**:

**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             |
|----------------------------------|--------------------|
| <a href="#">Firebox</a>          | 0 Users 0 Groups   |
| <a href="#">RADIUS</a>           | Primary Disabled   |
|                                  | Secondary Disabled |
| <a href="#">SecurID</a>          | Primary Disabled   |
|                                  | Secondary Disabled |
| <a href="#">LDAP</a>             | Primary Disabled   |
|                                  | Secondary Disabled |
| <a href="#">Active Directory</a> | 0 domains          |

- Under **Primary Server Settings** click **Enable RADIUS Server**:

**Fireware XTM Web UI**

User: admin | Help | Logout

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

Port

1812

Passphrase

Confirm

Timeout

5

seconds

Retries

3

- Complete **Primary Server Settings** form:

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

Hotspot

Servers

Settings

Users and Groups

Web Server Certificate

Single Sign-On

Terminal Services

VPN

SYSTEM

successfully accept and process RADIUS authentication requests.

**Primary Server Settings**

☒ Enable RADIUS Server

IP Address

Port

Passphrase

Confirm

Timeout  seconds

Retries

Group Attribute

Dead Time  Minutes

**Secondary Server Settings**

| 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. 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 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](https://[device interface IP address]/sslvpn_logon.shtml)

## User Management

There are several options for managing your users within LoginTC:

## Failover

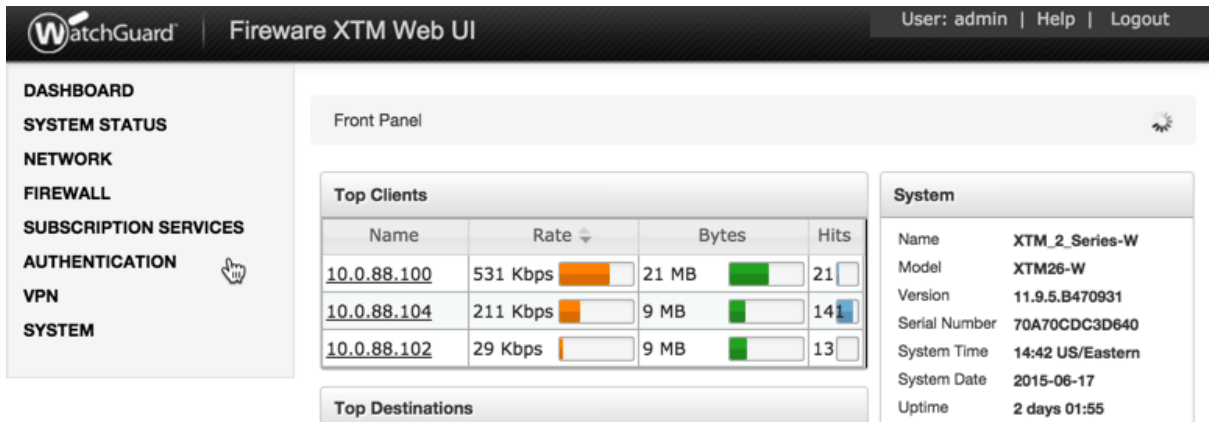
WatchGuard devices have built-in settings that make it easy to configure a secondary RADIUS server to provide failover.

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



The screenshot shows the WatchGuard Fireware XTM Web UI interface. The left-hand navigation bar has the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION (highlighted with a mouse cursor), VPN, and SYSTEM. The main content area is titled 'Front Panel' and contains two sections: 'Top Clients' and 'System'.

| Name                        | Rate     | Bytes | Hits |
|-----------------------------|----------|-------|------|
| <a href="#">10.0.88.100</a> | 531 Kbps | 21 MB | 21   |
| <a href="#">10.0.88.104</a> | 211 Kbps | 9 MB  | 14   |
| <a href="#">10.0.88.102</a> | 29 Kbps  | 9 MB  | 13   |

Below the 'Top Clients' table is a section for 'Top Destinations'. To the right of the 'Top Clients' table is the 'System' section, which displays the following information:

| 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**

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

Front Panel

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

### 3. Select **RADIUS**

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   |
| RADIUS  | 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

24

Hours

Secondary Server Settings

☒ Enable Secondary RADIUS Server

IP Address

Port

1812

Passphrase

Confirm

Timeout

5

seconds

Retries

3

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  Minutes 

| 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**

Retries

Group Attribute

Dead Time  Minutes 

## 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.

### 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:

**WatchGuard** | 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 |
|-----------------------------|----------|--------|------|
| <a href="#">10.0.88.104</a> | 166 Kbps | 11 MB  | 64   |
| <a href="#">10.0.88.100</a> | 107 Kbps | 720 KB | 37   |
| <a href="#">10.0.88.102</a> | 73 Kbps  | 9 MB   | 17   |

**Top Destinations**

**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         |

W

atchGuard

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 |
|-----------------------------|----------|--------|------|
| <a href="#">10.0.88.104</a> | 138 Kbps | 11 MB  | 57   |
| <a href="#">10.0.88.100</a> | 61 Kbps  | 873 KB | 36   |
| <a href="#">10.0.88.102</a> | 35 Kbps  | 10 MB  | 14   |

Top Destinations

| Name                           | Rate    | Bytes | Hits |
|--------------------------------|---------|-------|------|
| <a href="#">184.150.152.15</a> | 65 Kbps | 1 MB  | 3    |
| <a href="#">74.125.22.139</a>  | 53 Kbps | 2 MB  | 1    |
| <a href="#">10.0.10.164</a>    | 14 Kbps | 11 MB | 2    |

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

Reboot

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: rcvcd cmd=1 'toSessiond/updateActivity' fromIPC=61236

2015-06-17 15:03:23 sessiond sessiond: get into sess\_prce\_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 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff:62 WPA: pairwise key handshake completed (RSN)

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: rcvcd 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

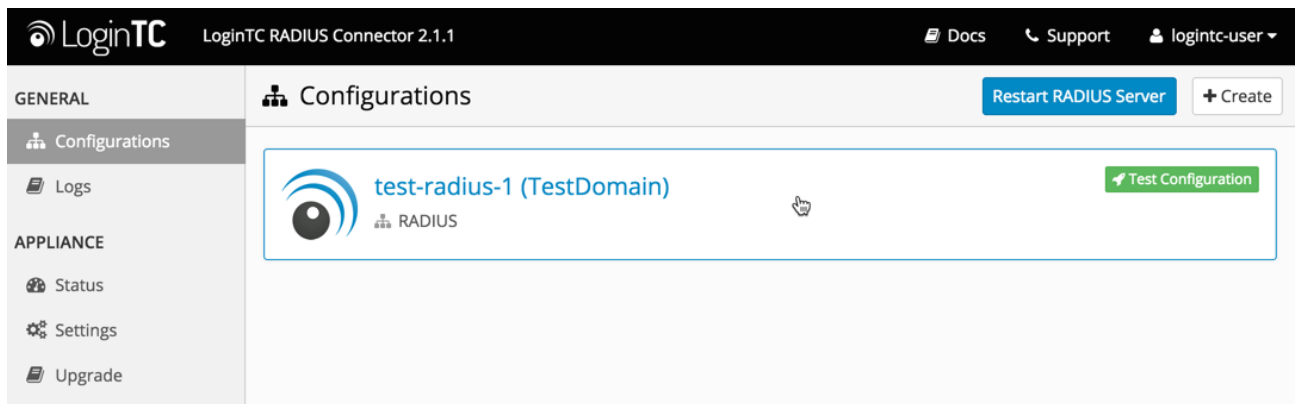
settings:

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

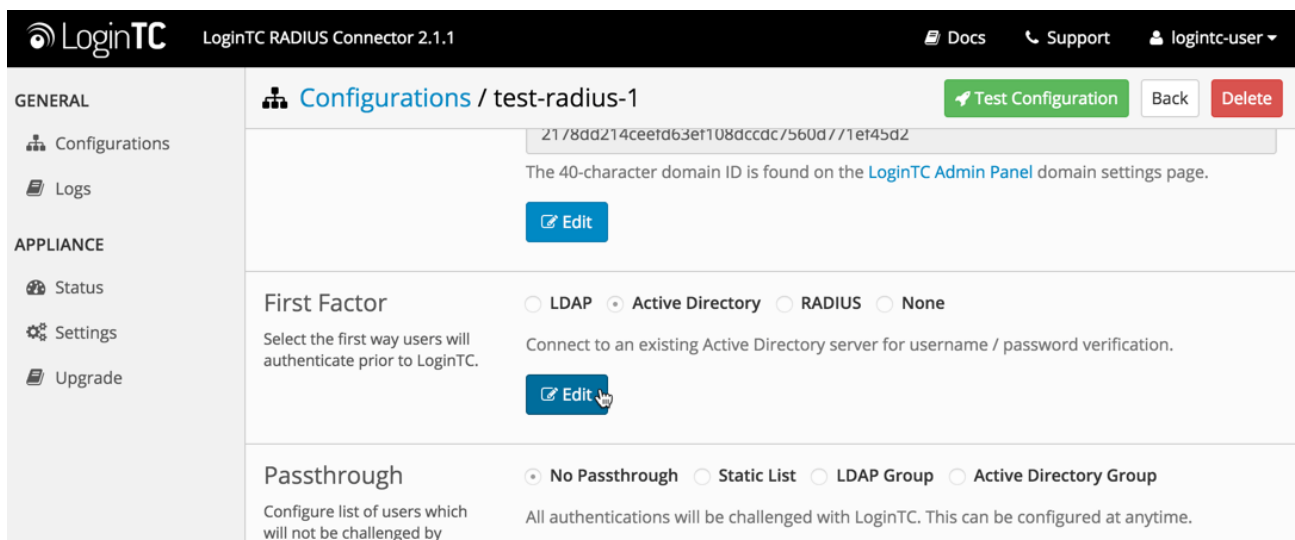
Search for the following error message:

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

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**Edit Configuration / First Factor** Cancel

The attribute containing the user's email address. Examples: mail or email.

**Group Attribute (Advanced)**  
Specify an additional user group attribute to be returned the authenticating server.

☒ None ☐ Specify a Group Attribute  
Do not send additional Group Attribute information (default).

**Connection Encryption**  
☒ None ☐ SSL ☐ STARTTLS  
No connection encryption.

- 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.

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**Edit Configuration / First Factor** Cancel

The attribute containing the user's email address. Examples: mail or email.

**Group Attribute (Advanced)**  
Specify an additional user group attribute to be returned the authenticating server.

☐ None ☒ Specify a Group Attribute

**RADIUS Group Attribute**  
filter-id  
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.

**AD Group**  
SSLVPN-Users  
The name of the AD 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.

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** :

Fireware XTM Web UI

User: admin | Help | Logout

DASHBOARD

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

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

Traffic Monitor

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)\*\*\*\*\* RECV an IKE packet at 10.0.10.8:500(socket=

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)ike\_match\_if\_name: Match pcy [RandomR\_mu] dev=a

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)ike\_match\_if\_name: Match pcy [L2TP-IPSec\_I2] dev=a

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)Found IKE Policy [RandomR\_mu, dev=anyE] for peer

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)IkeNotifyPayloadNtoH : SPI Size 16 first4(0x95b52557

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)Process Notify Payload : NOTIFY-TYPE : 36136

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)Process ISAKMP Notify : from peer 0x0a00a8c proto

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)Received DPD R\_U\_THERE message from 10.0.10.14

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)IkeInNotifyProcess: gateway is UP (peerIp=10.0.10.14

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)ike\_p1\_status\_chg: ikePcyName=RandomR\_mu, statu

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)ikeMultiWanVpnFailBack: -->

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)MWAN-Failback muvpn case, do nothing - name=Ran

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)IkeNotifyPayloadHtoN : net order spi(0x95 0xb5 0x25 0

2015-06-17 15:04:23iked (10.0.10.8<->10.0.10.140)Sending DPD R\_U\_THERE\_ACK message to 10.0.10

2015-06-17 15:04:43iked \*\*\*\*\* RECV message on fd\_server(7) \*\*\*\*\*

2015-06-17 15:04:43iked recv CMD XPATH(/ping), need to process it

Click on the **Authentication** tab:

Fireware XTM Web UI

User: admin | Help | Logout

DASHBOARD

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

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

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

10.0.10.83

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.

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

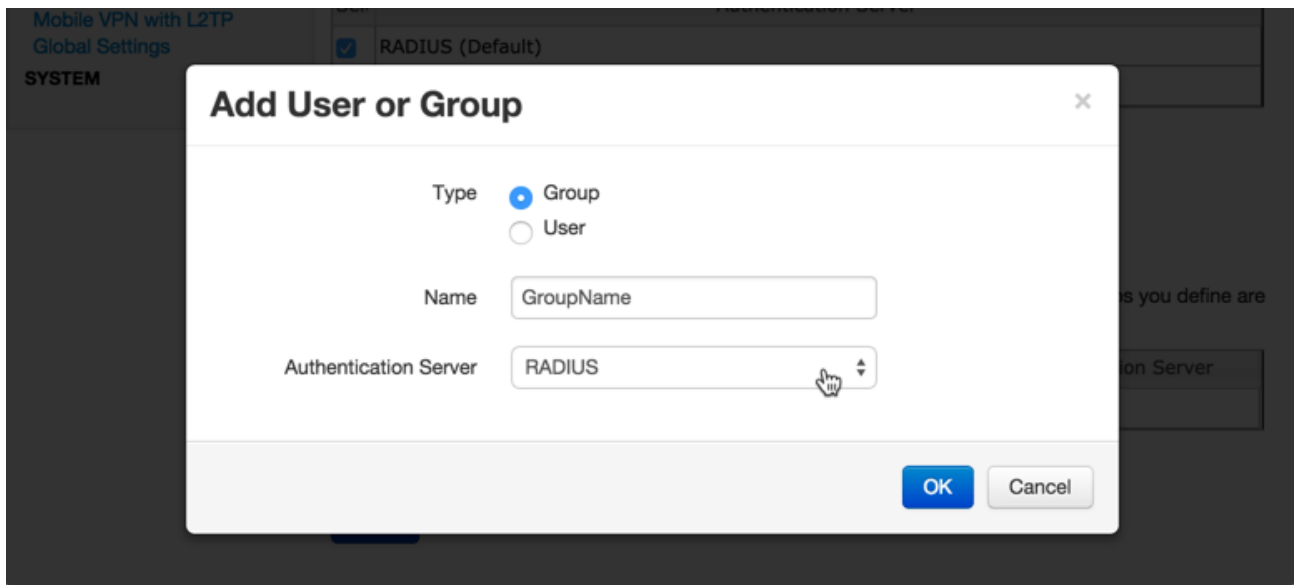
Add

Remove

Save

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

29/32



## 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**

| 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   |

|               |                  |
|---------------|------------------|
| 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**

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

Front Panel

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**

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   |
| RADIUS  | 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 10 seconds longer than the LoginTC Request Timeout set in the LoginTC RAIDUS Connector.

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 / 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

Port

Passphrase

Confirm

Timeout  seconds  
Range: 1-120 Default: 5

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?](#)

## Email Support

For any additional help please email [support@cyphercor.com](mailto:support@cyphercor.com). Expect a speedy reply.