

# WatchGuard XTM and Firebox IPSec 2FA

[logintc.com/docs/connectors/watchguard-ipsec](https://logintc.com/docs/connectors/watchguard-ipsec)



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 XTM and Firebox IPSec Alternative](#).

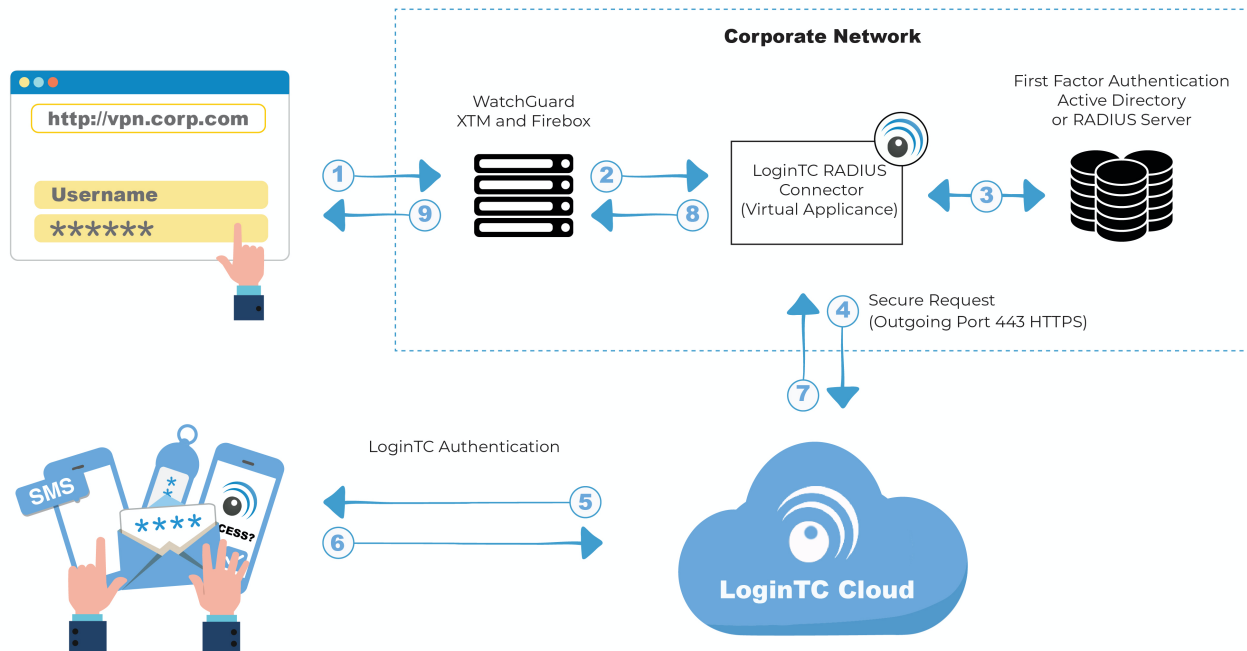
## User Experience

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).

## Video Instructions

Watch Video At: <https://youtu.be/mDQ9HdCqYK8>

## Architecture



## Authentication Flow

1. A user attempts access with their existing WatchGuard client with username / password
2. A RADIUS authentication request is sent to the LoginTC RADIUS Connector
3. The username / password is verified against an existing first factor directory (LDAP, Active Directory or RADIUS)
4. An authentication request is made to LoginTC Cloud Services
5. Secure push notification request sent to the user's mobile or desktop device
6. User response (approval or denial of request) sent to LoginTC Cloud Services
7. The LoginTC RADIUS Connector polls until the user responds or a timeout is reached
8. RADIUS Access-Accept sent back to WatchGuard
9. User is granted access to WatchGuard

## Compatibility

WatchGuard appliance compatibility:

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

## Appliance not listed?

We probably support it. [Contact us](#) if you have any questions.

## Compatibility Guide

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

## Prerequisites

Before proceeding, please ensure you have the following:

- [LoginTC Admin Panel](#) account
- Computer virtualization software such as [VMware ESXi](#), [VirtualBox](#), or [Hyper-V](#)
- Virtual Machine requirements:
  - 2048 MB RAM
  - 8 GB disk size

## Create Application

Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

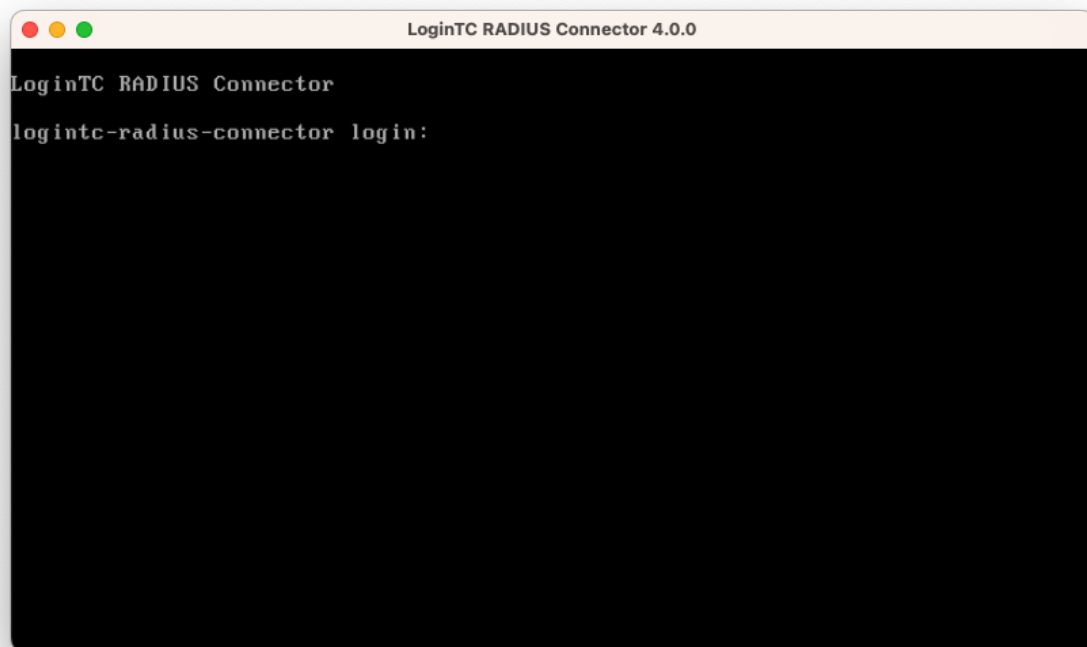
Create a LoginTC Application in [LoginTC Admin Panel](#), follow [Create Application Steps](#).

If you have already created a LoginTC Application for your deployment, then you may skip this section and proceed to [Installation](#).

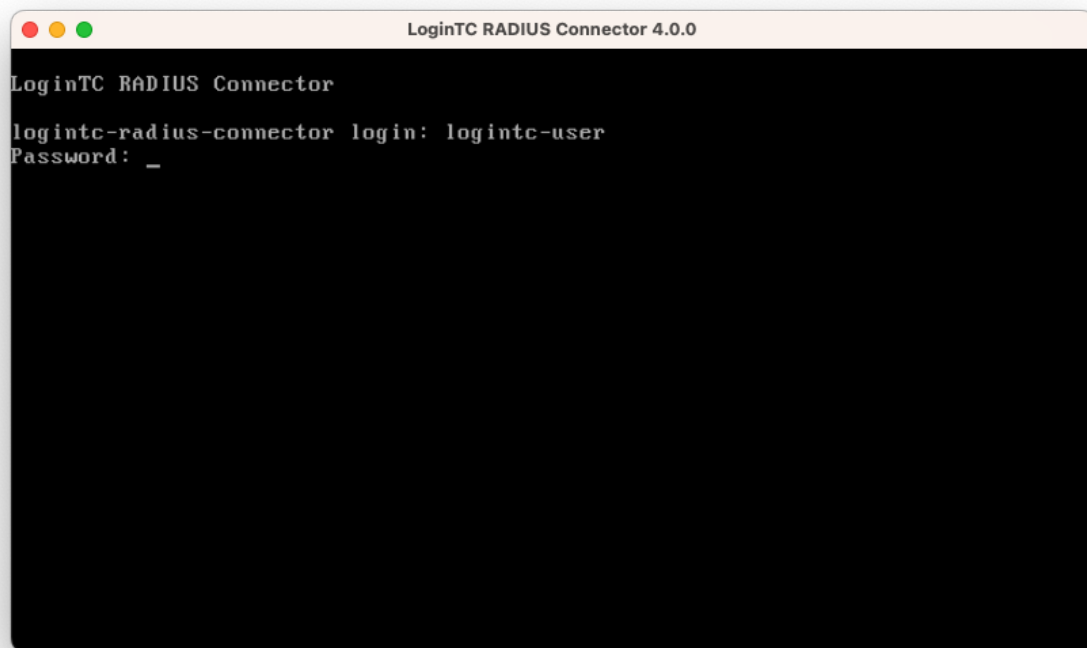
## Installation

1. Import the virtual appliance your computer virtualization software  
[Instructions for Hyper-V](#)
2. Ensure that LoginTC RADIUS CONNECTOR has a virtual network card
3. Start the virtual appliance

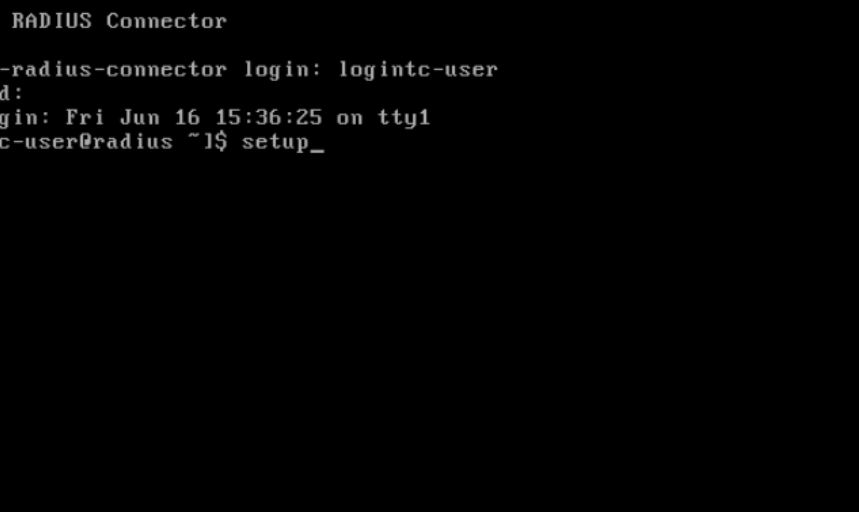
4. You will be with a console prompt:



5. Login using the username **logintc-user** and default password **logintcradius**:



6. Once logged in type **setup**:



macOS window titled "LoginTC RADIUS Connector 4.0.0". The window has standard macOS window controls (red, yellow, green buttons) and a title bar. A hint "To release your mouse press: Control-⌘" is visible in the top right corner.

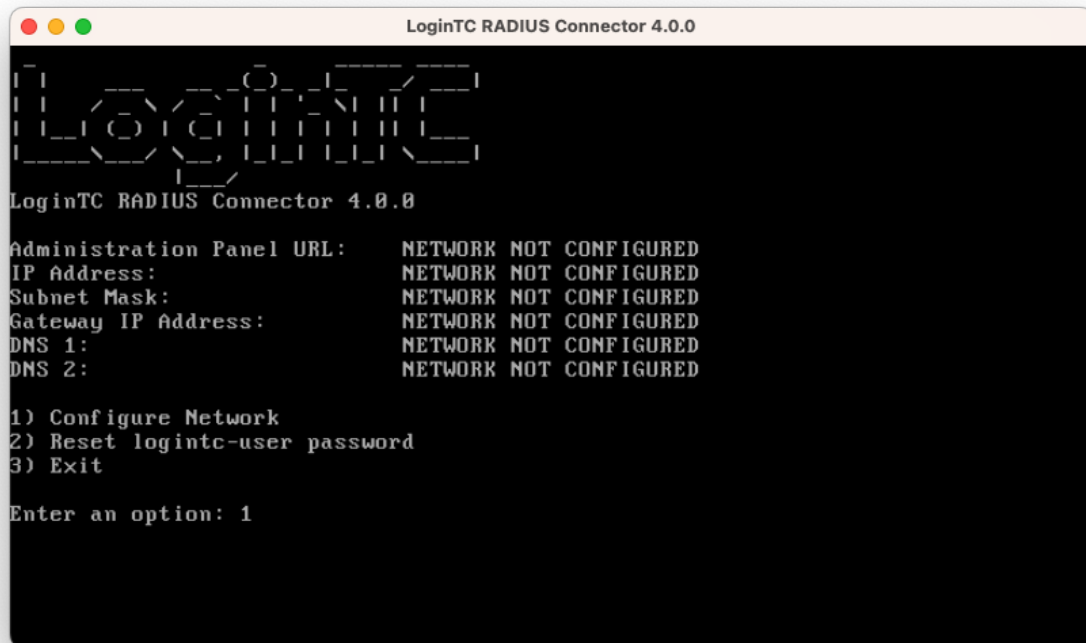
```
LoginTC RADIUS Connector

logintc-radius-connector login: logintc-user
Password:
Last login: Fri Jun 16 15:36:25 on tty1
[logintc-user@radius ~]$ setup_
```

7. Follow the on-screen prompt to setup a new password for **logintc-user**:

[illegible]

8. By default the appliance network is not configured. Manually configure the network by typing **1** and hit enter:



```
LoginTC RADIUS Connector 4.0.0

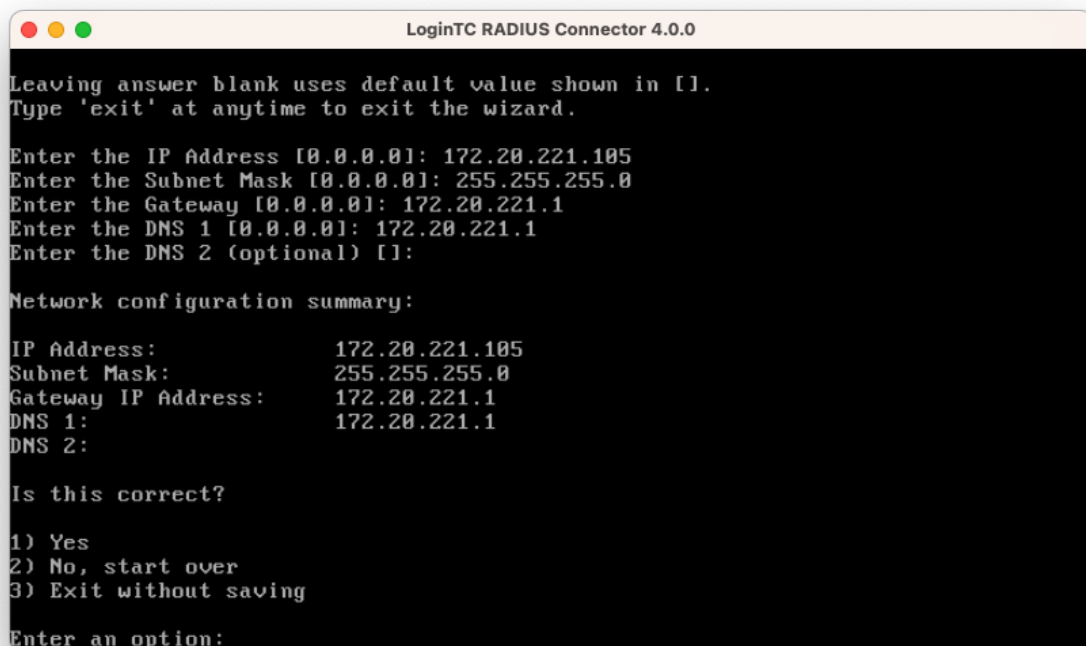
LoginTC RADIUS Connector 4.0.0

Administration Panel URL:  NETWORK NOT CONFIGURED
IP Address:                NETWORK NOT CONFIGURED
Subnet Mask:               NETWORK NOT CONFIGURED
Gateway IP Address:       NETWORK NOT CONFIGURED
DNS 1:                    NETWORK NOT CONFIGURED
DNS 2:                    NETWORK NOT CONFIGURED

1) Configure Network
2) Reset logintc-user password
3) Exit

Enter an option: 1
```

9. Follow the on-screen prompts to setup the network. When done, type **1** and enter to confirm the settings:



```
LoginTC RADIUS Connector 4.0.0

Leaving answer blank uses default value shown in [].
Type 'exit' at anytime to exit the wizard.

Enter the IP Address [0.0.0.0]: 172.20.221.105
Enter the Subnet Mask [0.0.0.0]: 255.255.255.0
Enter the Gateway [0.0.0.0]: 172.20.221.1
Enter the DNS 1 [0.0.0.0]: 172.20.221.1
Enter the DNS 2 (optional) []:

Network configuration summary:

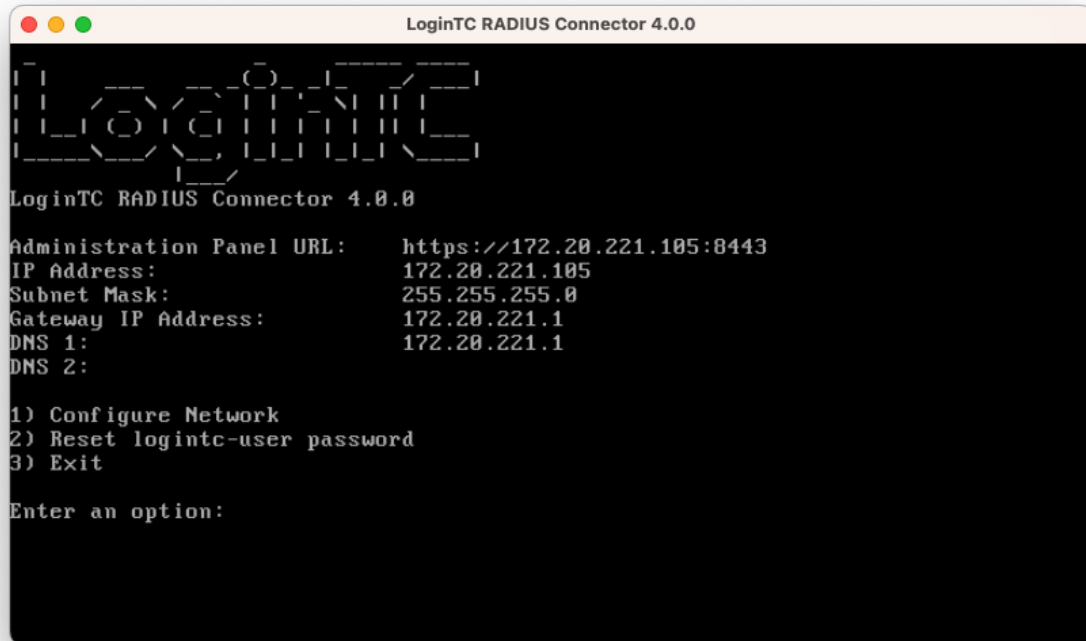
IP Address:                172.20.221.105
Subnet Mask:               255.255.255.0
Gateway IP Address:       172.20.221.1
DNS 1:                    172.20.221.1
DNS 2:

Is this correct?

1) Yes
2) No, start over
3) Exit without saving

Enter an option: 1
```

10. You will be presented with the network configuration which includes the URL to connect to the appliance from a web browser (example <https://172.20.221.105:8443>):



```

LoginTC RADIUS Connector 4.0.0

LoginTC
LoginTC RADIUS Connector 4.0.0

Administration Panel URL:  https://172.20.221.105:8443
IP Address:                172.20.221.105
Subnet Mask:               255.255.255.0
Gateway IP Address:        172.20.221.1
DNS 1:                     172.20.221.1
DNS 2:

1) Configure Network
2) Reset logintc-user password
3) Exit

Enter an option:
```

11. Navigate to the URL shown in the console dashboard (example: <https://172.20.221.105:8443>):
- 



**LoginTC RADIUS Connector**

**Username**

**Password**

**Log in**

Version 0.1.0-SNAPSHOT



12. Login using the username **logintc-user** and the password that was set in the initial setup:
- 



LoginTC RADIUS Connector

Username

logintc-user

Password

\*\*\*\*\*

Log in

Version 0.1.0-SNAPSHOT

13. Link to your existing LoginTC organization. The 64-character Organization API Key is found on the LoginTC Admin Panel under **Settings** >page **API** >page **Click to view**, also see [Organization API Key](#):
- 



Welcome to LoginTC RADIUS Connector!

Organization API Key

The 64-character organization API key is found on the LoginTC Admin Panel Settings page.

[Change LoginTC API Host](#)

HTTP Proxy ☐ Enabled ☒ Disabled

Next

[Log out](#)

14. Confirm the LoginTC organization name and click **Continue to LoginTC RADIUS Connector**:
- 



Organization Found:

Example Inc.

Continue to LoginTC RADIUS Connector

[Log out](#)

15. If you have an existing LoginTC RADIUS Connector you wish to import configurations then click **Yes, import configurations from an existing LoginTC RADIUS Connector**, otherwise click **No, continue to the administration panel**:
- 



#### Import configuration from an existing LoginTC RADIUS Connector?

If you have already deployed an older version of the LoginTC RADIUS Connector then you can attempt to import the configurations. The criteria for a successful import are:

- ☒ Network Connectivity
- ☒ Valid account credentials
- ☒ LoginTC RADIUS Connector v2.7.1 - v3.0.7
- ☒ Configurations using Applications (not Domains)

Yes, import configurations from an existing LoginTC RADIUS Connector

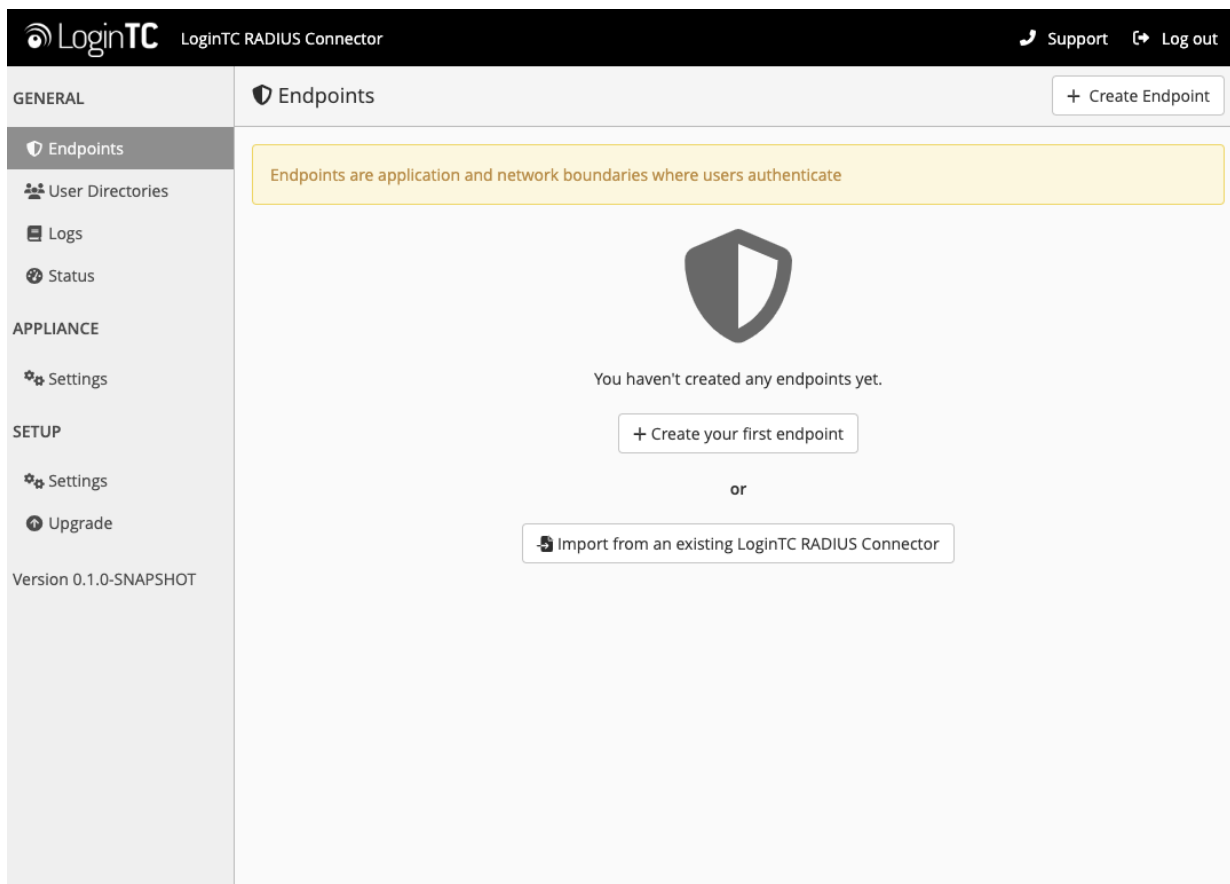
No, continue to the administration panel

[Log out](#)

#### NOTE

These instructions assume a new environment. For a complete 2.X / 3.X to 4.X upgrade guide: [LoginTC RADIUS Connector Upgrade Guide](#)

16. Now you are ready to use the LoginTC RADIUS Connector:



The LoginTC RADIUS Connector runs Linux with SELinux. A firewall runs with the following open ports:

Port	Protocol	Purpose
1812	UDP	RADIUS authentication
443	TCP	API traffic
8443	TCP	Web interface
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.

## Configuration

Endpoints describe how the appliance will authenticate your RADIUS-speaking device with an optional first factor and LoginTC as a second factor. Each endpoint has **4 Sections**:

### 1. LoginTC Settings

This section describes how the appliance itself authenticates against LoginTC Admin Panel with your LoginTC Application. Only users that are part of your organization and added to the domain configured will be able to authenticate.

## 2. User Directory

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.

## 3. Challenge Strategy / 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 Settings

This section describes which RADIUS-speaking device will be connecting to the appliance and whether to encrypt API Key, password and secret parameters.

The **web interface** makes setting up an endpoint 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 Endpoint

---

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 endpoint file by clicking **+ Create your first endpoint:**

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints

Create Endpoint

Endpoints are application and network boundaries where users authenticate

You haven't created any endpoints yet.

Create your first endpoint

or

Import from an existing LoginTC RADIUS Connector

## LoginTC Settings

A list of available Applications will be displayed from your LoginTC organization. Select which LoginTC **Application** to use:

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade


Version 4.0.0

Endpoints / Create / LoginTC Application

Step 1 of 4


Cancel

Select an application from your LoginTC organization. Applications dictate which domain and policies are used.




Cisco ASA SSL VPN

Cisco ASA SSL VPN Example Inc. Secure Access




Fortinet FortiGate SSL VPN

Fortinet FortiGate SSL VPN Example Inc. Secure Access




Generic AD FS

Generic AD FS Example Inc. Secure Access



Generic RADIUS

Generic RADIUS Example Inc. Secure Access



Microsoft OWA

Configure the application:

16/61



LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints / Create / LoginTC Application

Step 1 of 4
Back
Cancel

Endpoints

User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

Generic RADIUS

Generic RADIUS
Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

The 40-character Application ID is found on the LoginTC Admin Panel Application page.

Application API Key

79EPAK5OgrVEK1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDI24D9V1

The 64-character Application API key is found on the LoginTC Admin Panel Application page.

Request Timeout

Request Timeout

60

The amount of time in seconds the LoginTC RADIUS Connector should poll for a user to respond. The value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

IP Address

The IP Address will be shown to the end user prior to approving the request. The corresponding LoginTC domain will need to be configured with an IP Address domain attribute.

☒ Yes, send IP Address of the originating request when available
☐ No, do not send IP Address of originating request

RADIUS Attribute Name

Calling-Station-Id

The RADIUS attribute used by the VPN client to send the client IP Address.

Test
Next

Click Test before continuing.

Configuration values:

Property	Explanation
Application ID	The 40-character Application ID, <a href="#">retrieve Application ID</a>
Application API Key	The 64-character Application API Key, <a href="#">retrieve Application API Key</a>
Request Timeout	Number of seconds that the RADIUS connector will wait for


The Application ID and Application API Key are found on the [LoginTC Admin Panel](#).

## Request Timeout

17/61

Make a note of what you set the Request Timeout to as you will need to use a larger timeout value in your RADIUS client. 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 RADIUS Client. For more information see: [Recommended settings for an optimal user experience for VPN access](#)

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

 LoginTC RADIUS Connector

[Support](#) [Log out](#)

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP


Settings

Upgrade

Version 4.0.0

Endpoints / Create / LoginTC Application

Step 1 of 4 Back Cancel

 Generic RADIUS

Generic RADIUS

Generic RADIUS Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

The 40-character Application ID is found on the LoginTC Admin Panel Application page.

Application API Key

79EPAK5OgrVEk1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDI24D9V1

The 64-character Application API key is found on the LoginTC Admin Panel Application page.

Request Timeout

Request Timeout

60

The amount of time in seconds the LoginTC RADIUS Connector should poll for a user to respond. The value should be 10 seconds shorter than the timeout in your RADIUS client (e.g. VPN). For example if the VPN timeout is 90 seconds, this value should be no longer than 80 seconds.

IP Address

The IP Address will be shown to the end user prior to approving the request. The corresponding LoginTC domain will need to be configured with an IP Address domain attribute.

☒ Yes, send IP Address of the originating request when available

☐ No, do not send IP Address of originating request

RADIUS Attribute Name

Calling-Station-Id

The RADIUS attribute used by the VPN client to send the client IP Address.

Test Next

Test successful, click Next to continue.

## User Directory

Configure the user directory to be used for first authentication factor 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

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints / Create / User Directory

Step 2 of 4BackCancel

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Select a user directory to leverage for username and password authentication

Active Directory

Leverage your Active Directory.

L

Generic LDAP

Leverage your LDAP server.

R

Generic RADIUS

Leverage your RADIUS server.

or

Continue without a User Directory

Users will not be challenged with password authentication. (Can be changed at any time)

## Active Directory / Generic LDAP Option

Select **Active Directory** if you have an AD Server. For all other LDAP-speaking directory services, such as OpenDJ or OpenLDAP, select **Generic LDAP**:

19/61

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

User Directories / Create / Configure Active Directory Server

Step 2 of 2
Back
Cancel

Connection Details

Name (optional)

Active Directory Server

Name of the Active Directory server.

IP Address or Host Name

The IP address or host name of the Active Directory Server.

Port (optional)

389

The default is 389 for LDAP and 636 for LDAPS (LDAP + SSL).

☒ No connection encryption
☐ SSL
☐ STARTTLS

Bind Details

How to authenticate against Active Directory to verify a username and password.

☒ Bind with credentials
☐ Anonymous

Bind DN

DN of an account with read access to the directory. Example: cn=admin,dc=example,dc=com.

Bind Password

The password for the above Bind DN account.

Query Details

Where and how to find relevant user entries.

Base DN

The top-level DN that usernames will be queried from. Example: dc=example,dc=com.

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

20/61

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>
<code>LDAP Group</code> (optional)	The name of the LDAP group to be sent back to the authenticating server.	<code>SSLVPN-Users</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>

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

### Group Attribute and Access Control

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

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.

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints / Create / User Directory / Group Attribute

Step 2 of 4BackCancel

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Group Attribute

None

Specify a Group attribute

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

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 of value 11, use: Filter-Id

Groups

SSLVPN-Users

A comma delimited list of names of possible user directory groups to be sent back to the authentication 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. Examples: SSLVPN-Users or Administrators,Sales,Engineers.

TestNext

Click Test before continuing.

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**:

22/61

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

User Directories / Create / Configure RADIUS Server

Step 2 of 2
Back
Cancel

RADIUS Server Details

Name (optional)

Generic RADIUS Server

Name of the RADIUS server.

IP Address or Host Name
The IP address or host name of the RADIUS Server.

Authentication Port

1812

The authentication port of the RADIUS server.

Shared Secret
The RADIUS shared secret.

Test
Create

Click Test before continuing.

Configuration values:

Property	Explanation	Examples
IP Address or Host Name	Host or IP address of the RADIUS server	radius.example.com or 192.168.1.43
Authentication Port (optional)	Port if the RADIUS server uses non-standard (i.e., 1812)	1812
Shared Secret	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	testing123

## RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) returned by the RADIUS server will be relayed.

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

## Challenge Strategy / 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.

The screenshot shows the 'LoginTC RADIUS Connector' interface. The top navigation bar includes the LoginTC logo, 'LoginTC RADIUS Connector', and links for 'Support' and 'Log out'. The main header indicates the current page is 'Endpoints / Create / Challenge Strategy', with 'Step 3 of 4' and 'Back'/'Cancel' buttons. A left sidebar contains navigation links: 'GENERAL', 'Endpoints', 'User Directories', 'Logs', 'Status', 'APPLIANCE', 'Settings', 'SETUP', 'Settings', 'Upgrade', and 'Version 4.0.0'. The main content area has a yellow instruction box: 'Select which users should be challenged with LoginTC and which should bypass LoginTC'. Below this are three selectable options, each with an icon and a description: 1. 'Challenge All Users' (checkmark icon) with the description 'All users will be challenged with LoginTC.' 2. 'Challenge Users Based on Static Username List' (document icon) with the description 'Only users in a static username list will be challenged with LoginTC.' 3. 'Challenge Users Based on Group Membership' (group of people icon) with the description 'Leverage Active Directory and LDAP Group Membership to determine which users are challenged with LoginTC and which users bypass LoginTC.'

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.

### Challenge All Users

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

### Challenge Users Based on Static Username 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
 Support
Log out

GENERAL

Endpoints

User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

Endpoints / Create / Challenge Strategy

Step 3 of 4
Back
Cancel

Static Username List

Only users in a static username list will be challenged with LoginTC.

Challenge Users

Enter a newline separated list of usernames that will be challenged with LoginTC. Users not in this list will bypass LoginTC. Example:

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

Test
Next

Click Test before continuing.

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

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

## Challenge Users Based on Group Membership

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.

25/61

LoginTC RADIUS Connector

Support
Log out

GENERAL
Endpoints / Create / Challenge Strategy

Step 3 of 4
Back
Cancel

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade
Version 4.0.0

Group Membership

Precedence is always given to bypass groups when both challenge and bypass groups are specified.

Challenge Groups

Comma separated list of groups whose users will be challenged with LoginTC. Example: 2FA Users

Bypass Groups

Comma separated list of groups whose users will always bypass LoginTC. Example: No 2FA Users

Test
Next

Click Test before continuing.

Configuration values:

Property	Explanation	Examples
Challenge Groups (Optional)	Comma separated list of groups for which users will be challenged with LoginTC	SSLVPN-Users or two-factor-users
Challenge Groups (Optional)	Comma separated list of groups for which users will always bypass LoginTC	NOMFA-Users

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

## Client Settings

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

26/61

LoginTC RADIUS Connector
 Support Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade
Version 4.0.0

Endpoints / Create / Client Settings

Step 4 of 4
Back
Cancel

Generic RADIUS Details

Name (optional)

Name for the endpoint.

IP Address
+

The IP Address or IPv4 CIDR Block of the Generic RADIUS. For example 192.168.0.1 or 192.168.0.0/16.

Shared Secret

The RADIUS shared secret.

Authentication Mode
☒ Direct
☐ Iframe
☐ Challenge
☐ Challenge Interactive

How the LoginTC authentication is performed
Send authentication request directly and automatically.

Client configuration values:

Property	Explanation	Examples
name	A unique identifier of your RADIUS client	CorporateVPN
IP Addresss	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN). Add additional IP Addresses by clicking <b>plus</b> .	192.168.1.44
Shared Secret	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret

Under Authentication Mode select **Challenge**

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

Endpoints / Create / Client Settings

Step 4 of 4
Back
Cancel

Generic RADIUS Details

Name (optional)

Generic RADIUS

Name for the endpoint.

IP Address

+

The IP Address or IPv4 CIDR Block of the Generic RADIUS. For example 192.168.0.1 or 192.168.0.0/16.

Shared Secret
The RADIUS shared secret.

Authentication Mode

☐ Direct
☐ Iframe
☒ Challenge
☐ Challenge Interactive

How the LoginTC authentication is performed

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.

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.

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

28/61

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints

Create Endpoint

Endpoints are application and network boundaries where users authenticate

Successfully created endpoint.

Generic RADIUS

Generic RADIUS (11.1.1.1)  
Generic RADIUS Example Inc. Secure Access

## Testing

When you are ready to test your configuration, create a LoginTC user (if you haven't already done so). The username should match your existing user. Provision a token by following the steps:

1. In a new tab / window log into the [LoginTC Admin Panel](#)
2. Click **Domains**
3. Click on your domain
4. Click on **Members**

Example Inc. Business

Docs
Support
administrator@example.com

GENERAL

Dashboard

Users

Applications

Policies

Groups

Bypass Codes

Devices

Phones

Hardware Tokens

User Logs

SETUP

Domains

Administrators

Admin Logs

Domains / Example Inc. Secure Access

Create Member

Members

Settings

Members

Example Inc. Secure Access has 88 member(s)

Create Member

View Members

Attributes

Example Inc. Secure Access doesn't have any domain attributes yet. [Learn more.](#)

Create Domain Attribute

Latest Actions

Action	User	Device/Phone	Domain	Group	Date
APPROVE_REQUEST_TEST	<a href="#">john.doe</a>	IOS-4f6aa853	Example Inc. Secure Access		<a href="#">4 seconds ago</a>
CREATE_REQUEST	<a href="#">john.doe</a>	IOS-4f6aa853	Example Inc. Secure Access		<a href="#">15 seconds ago</a>

5. Click **Issue Token** button beside your user:

The screenshot shows the LoginTC web interface. The top navigation bar includes the LoginTC logo, 'Example Inc.', 'Business', and links for 'Docs', 'Support', and 'administrator@example.com'. The left sidebar has a 'GENERAL' section with links to Dashboard, Users, Applications, Policies, Groups, Bypass Codes, Devices, Phones, Hardware Tokens, and User Logs. Below this is a 'SETUP' section with links to Domains, Administrators, and Admin Logs. The main content area is titled 'Domains / Example Inc. Secure Access / Members' and includes a '+ Create Member' button and a 'Settings' gear icon. Below the title are filters for 'State' (Any) and 'Filter', and a search bar. There are three buttons: 'Issue New Token' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). A message says 'Perform bulk action on 0 selected users'. A table lists users with columns for 'Username', 'State', 'Activation Code', and 'Actions'. The user 'john.doe' is listed with a state of 'Inactive' and a green '+ Issue Token' button in the Actions column.

Username	State	Activation Code	Actions
john.doe	Inactive		<a href="#">+ Issue Token</a>

6. A 10-character alphanumeric activation code will appear beside the user:

The screenshot shows the LoginTC web interface. The top navigation bar includes the LoginTC logo, 'Example Inc.', 'Business', and links for 'Docs', 'Support', and 'administrator@example.com'. The left sidebar has a 'GENERAL' section with links to Dashboard, Users, Applications, Policies, Groups, Bypass Codes, Devices, Phones, Hardware Tokens, and User Logs. Below this is a 'SETUP' section with links to Domains, Administrators, and Admin Logs. The main content area is titled 'Domains / Example Inc. Secure Access / Members' and includes a '+ Create Member' button and a 'Settings' gear icon. Below the title are filters for 'State' (Any) and 'Filter', and a search bar. There are three buttons: 'Issue New Token' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). A message says 'Perform bulk action on 0 selected users'. A table lists users with columns for 'Username', 'State', 'Activation Code', and 'Actions'. The user 'john.doe' is listed with a state of 'Pending' and an activation code 'HURRMUGUVH'. The Actions column shows a red 'Revoke Token' button.

Username	State	Activation Code	Actions
john.doe	Pending	HURRMUGUVH	<a href="#">Revoke Token</a>

7. Open the LoginTC mobile app.

8. Enter the 10-character alphanumeric activation code:

The screenshot shows a mobile application interface for adding a token. At the top, a status bar indicates 'No SIM', signal strength, time '2:28 PM', and battery level. Below this is a blue header bar with 'Cancel', 'Add Token', and 'Next' buttons. The main content area has a title 'Step 1 of 3: Enter Activation Code'. Below the title, the activation code 'HURRMUGUVH' is displayed. A text block explains that the 10-character alphanumeric activation code is supplied by the user's LoginTC-enabled service provider and that they should ask their administrator for one if they don't have one. At the bottom is a QWERTY keyboard with a 'Next' button to the right of the spacebar.

No SIM 2:28 PM

Cancel Add Token Next

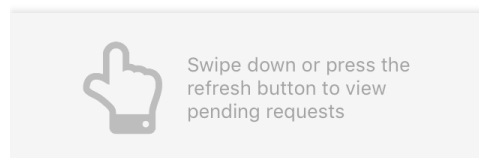
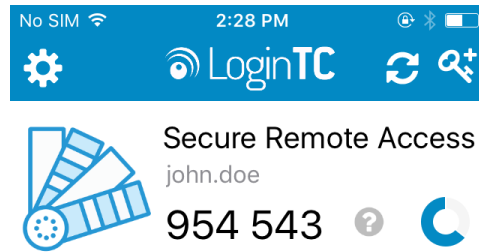
**Step 1 of 3: Enter Activation Code**

HURRMUGUVH

The 10-character alphanumeric activation code is supplied by your LoginTC-enabled service provider. If you don't already have an activation code, ask your administrator to issue you one.


Q W E R T Y U I O P  
A S D F G H J K L  
↑ Z X C V B N M ↵  
123 globe microphone space Next

## 9. Load the token to complete the process



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



 LoginTC RADIUS Connector

[Support](#) [Log out](#)

GENERAL

Endpoints / Generic RADIUS

Test Endpoint

Delete

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Read the Generic RADIUS [Documentation](#) to integrate your Generic RADIUS application with LoginTC.

Endpoint

Endpoint Name


Generic RADIUS

Edit

LoginTC Application

Application Name

Generic RADIUS




Application ID

3682ec813e2fd280032ad0cf57ec140923405391

Domain

Example Inc. Secure Access



Request Timeout

60

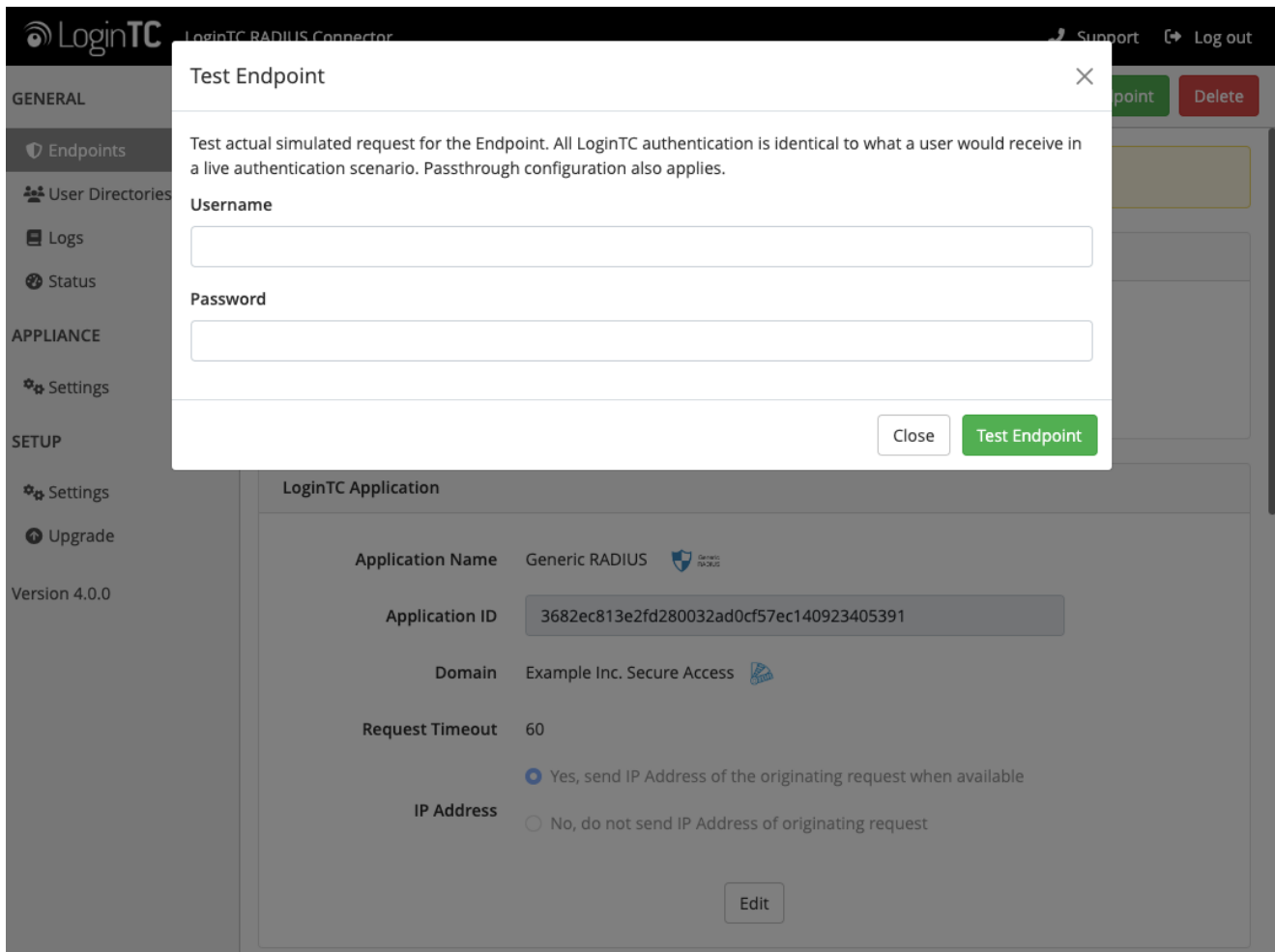
IP Address

☒ Yes, send IP Address of the originating request when available

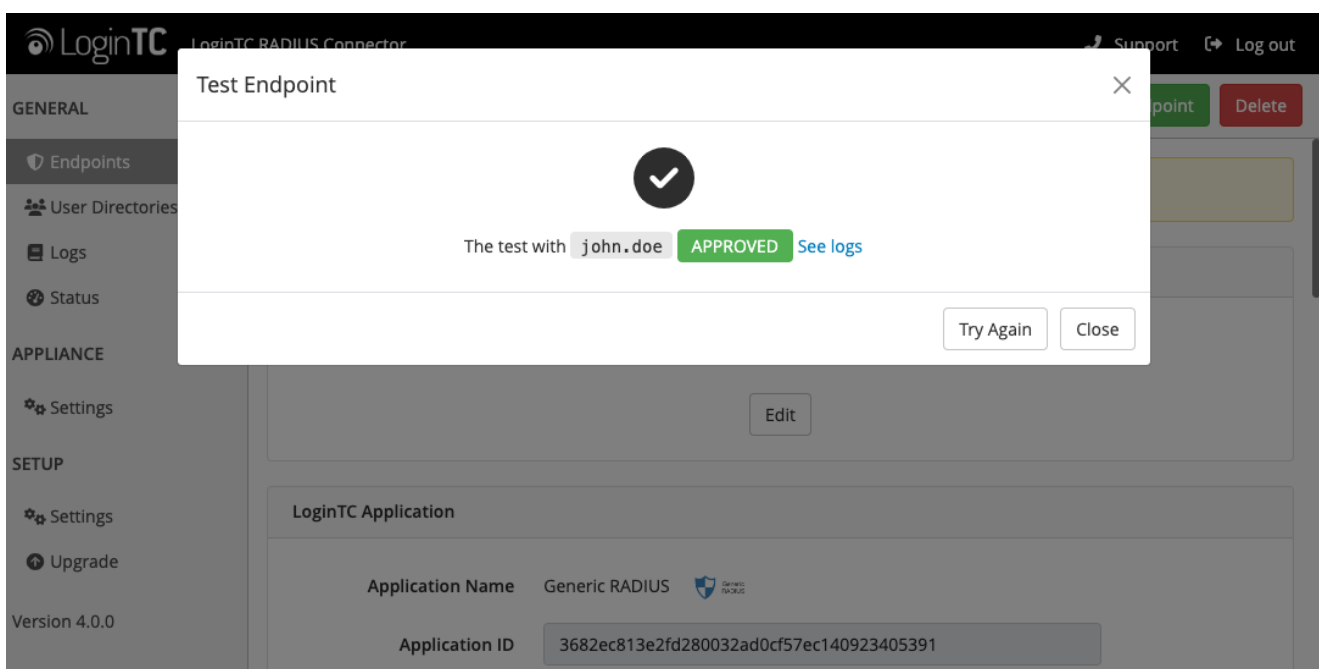
☐ No, do not send IP Address of originating request

Edit

Click **Test Configuration**:

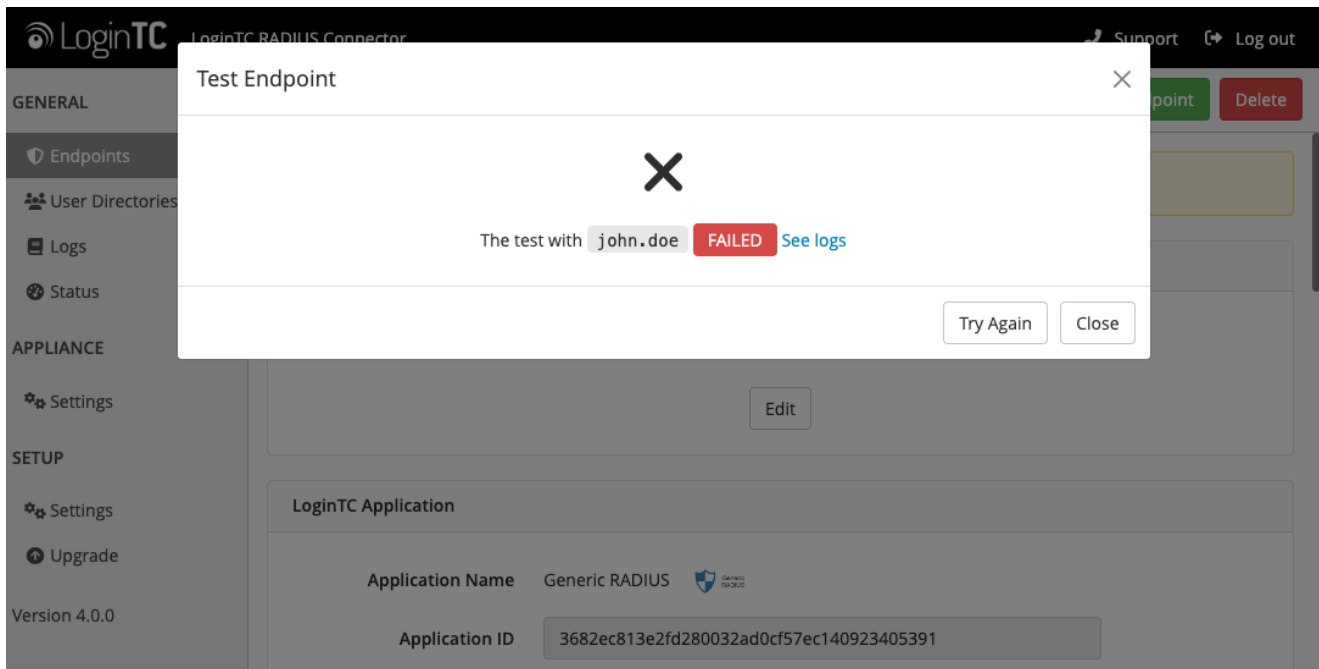


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

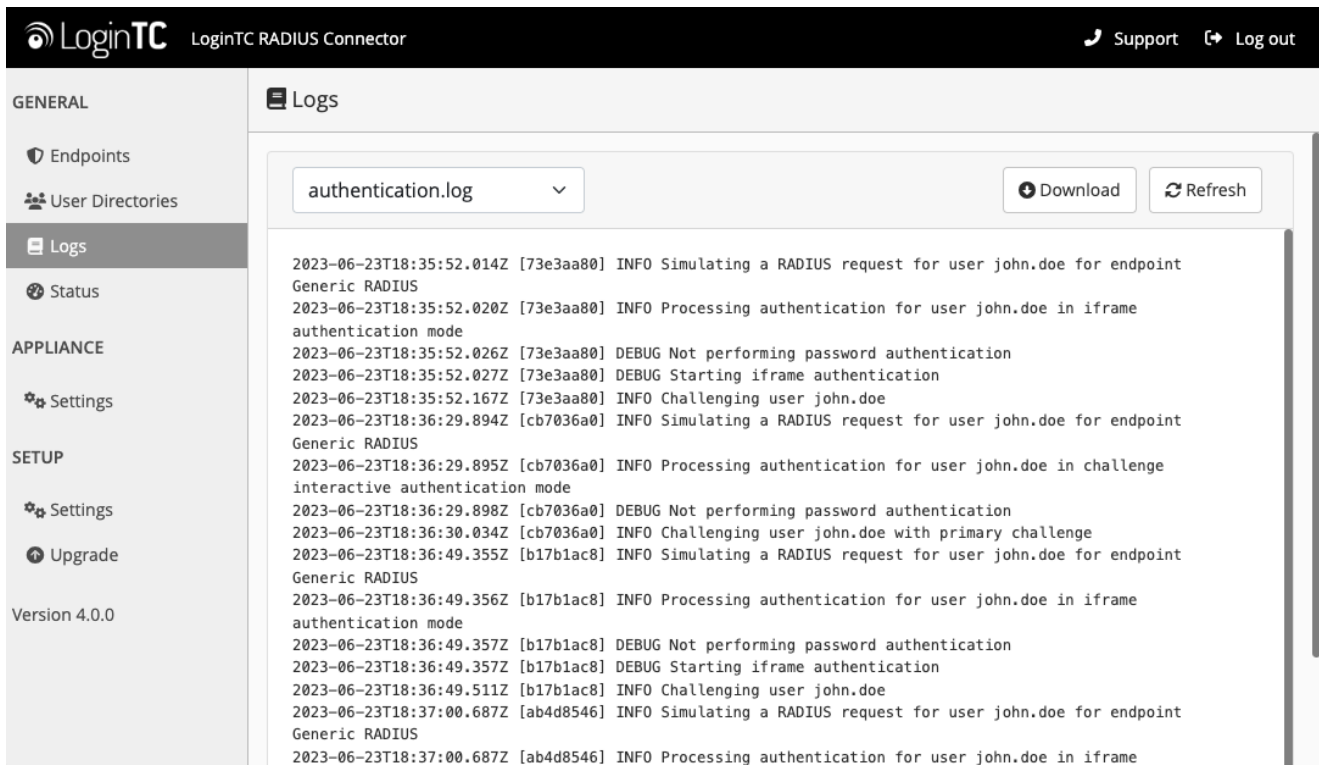


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



In this case, click **See logs** (or click the **Logs** section):



## 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 screenshot shows the 'Settings' page of the LoginTC RADIUS Connector. The page has a dark header with the LoginTC logo and 'LoginTC RADIUS Connector' text, along with 'Support' and 'Log out' links. A left sidebar contains navigation links: 'GENERAL' (Endpoints, User Directories, Logs, Status), 'APPLIANCE' (Settings), and 'SETUP' (Settings, Upgrade). The main content area is titled 'Settings' and contains two sections: 'RADIUS Details' and 'NTP Server'. The 'RADIUS Details' section shows 'IP Address' as 172.20.221.85 and 'RADIUS Authentication Port' as 1812. The 'NTP Server' section shows 'Enabled' with radio buttons for 'Yes' and 'No' (selected), and a message 'NTP is not enabled.' with an 'Edit' button.

RADIUS Details	
IP Address	172.20.221.85
RADIUS Authentication Port	1812

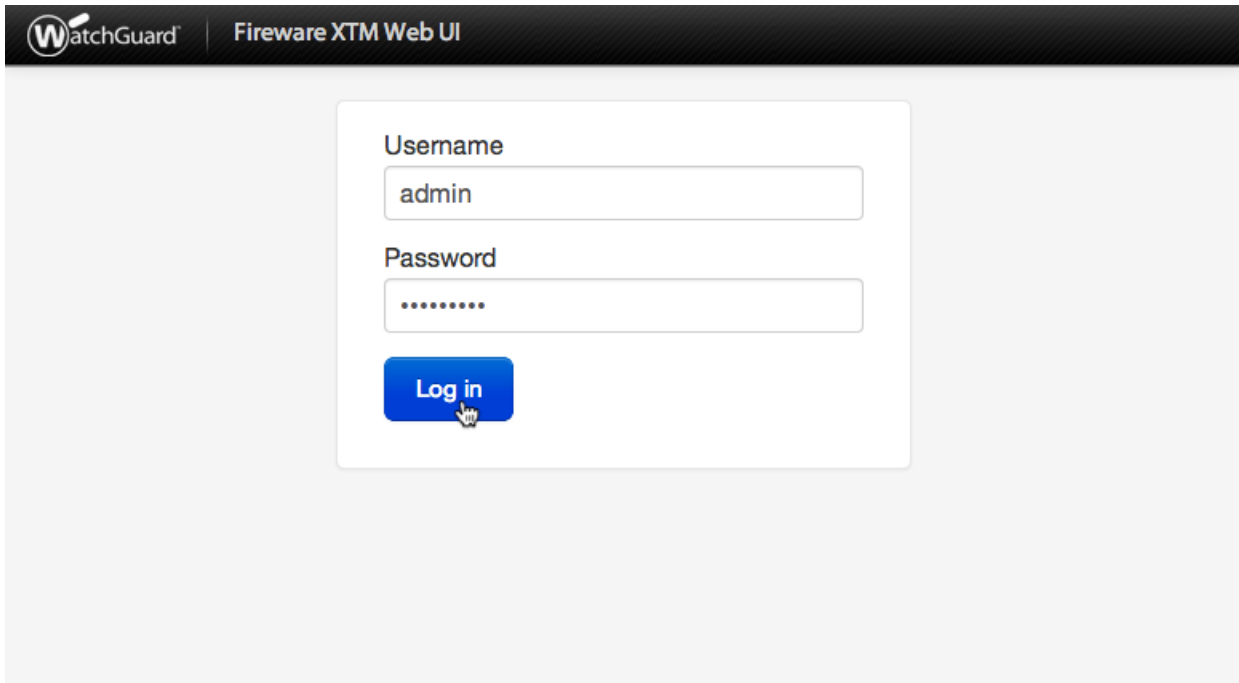
  

NTP Server	
Enabled	<input type="radio"/> Yes <input checked="" type="radio"/> No
NTP is not enabled.	
<button>Edit</button>	

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

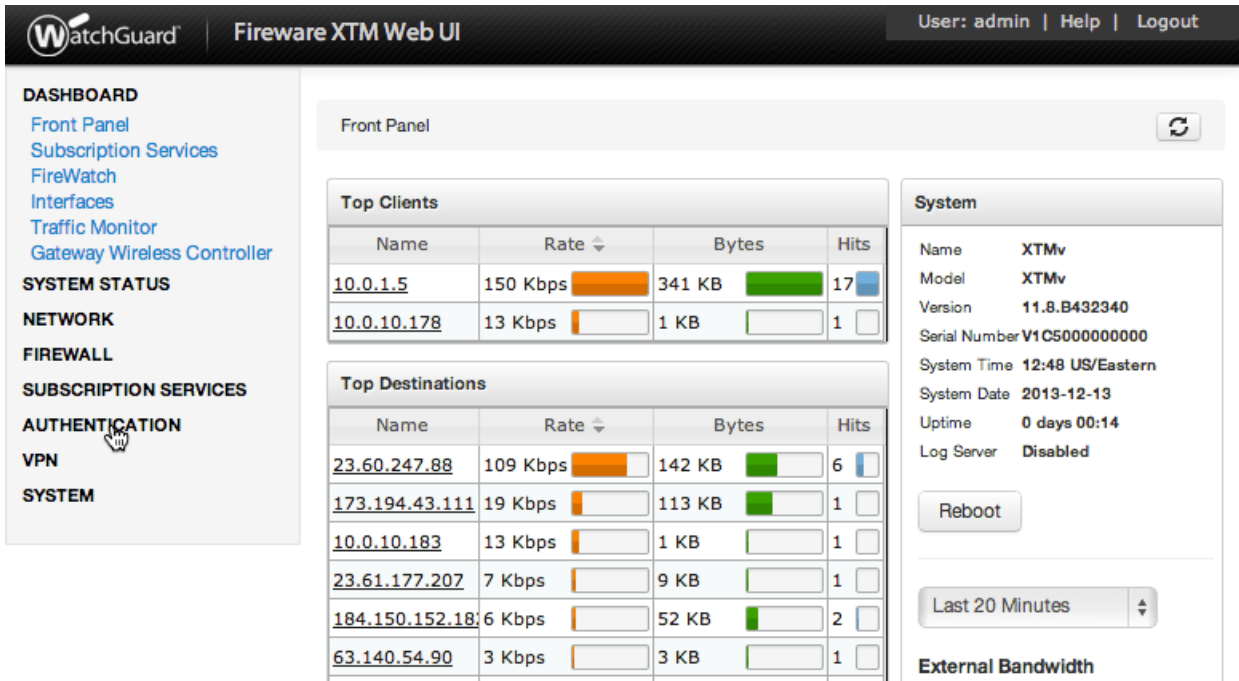
## Mobile VPN with IPsec

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



The screenshot shows the WatchGuard Fireware XTM Web UI login page. It features a dark header with the WatchGuard logo and the text "Fireware XTM Web UI". The main content area is light gray and contains a white login box. Inside the box, there are two input fields: "Username" with the text "admin" and "Password" with masked characters ".....". Below these fields is a blue "Log in" button with a mouse cursor hovering over it.

2. Click **Authentication**:



The screenshot shows the WatchGuard Fireware XTM Web UI dashboard. The top header includes the WatchGuard logo, "Fireware XTM Web UI", and user information "User: admin | Help | Logout". A left sidebar contains a navigation menu with categories: 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 includes a refresh button. It is divided into three sections: "Top Clients", "Top Destinations", and "System".

**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**:

**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
<a href="#">10.0.10.178</a>	13 Kbps	1 KB	1
<a href="#">10.0.1.5</a>	4 Kbps	58 KB	3

**Top Destinations**

Name	Rate	Bytes	Hits
<a href="#">10.0.10.183</a>	13 Kbps	1 KB	1
<a href="#">184.150.152.18</a>	2 Kbps	48 KB	1
<a href="#">66.196.113.5</a>	1 Kbps	4 KB	1
<a href="#">173.192.82.194</a>	208 bps	6 KB	1

**Top Policies**

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

**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**:

**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**

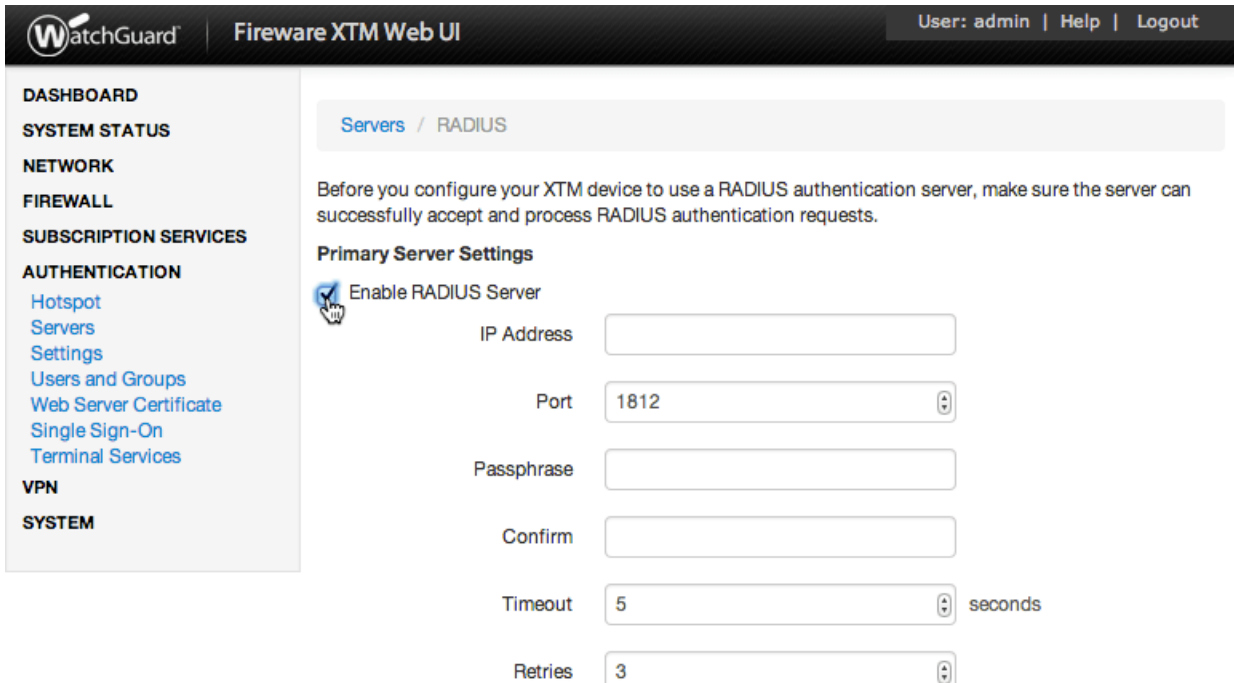
**SYSTEM**

**Servers**

**Authentication Servers**

Server	Status
<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

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



The screenshot shows the WatchGuard Fireware XTM Web UI interface. The top navigation bar includes the WatchGuard logo, the title "Fireware XTM Web UI", and user information "User: admin | Help | Logout". The left sidebar contains a menu with categories: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The "AUTHENTICATION" section is expanded, showing links for Hotspot, Servers, Settings, Users and Groups, Web Server Certificate, Single Sign-On, and Terminal Services. The main content area is titled "Servers / RADIUS" and contains a warning message: "Before you configure your XTM device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests." Below this is the "Primary Server Settings" section, which includes a checkbox labeled "Enable RADIUS Server" that is checked. To the right of the checkbox are input fields for "IP Address", "Port" (set to 1812), "Passphrase", "Confirm", "Timeout" (set to 5 seconds), and "Retries" (set to 3).

**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 / 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

Retries

## 6. 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

10.0.10.130

Port

1812

Passphrase

\*\*\*\*\*

Confirm

\*\*\*\*\*

Timeout

60

seconds

Retries

1

Group Attribute

11

Dead Time

10

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	0

### Group Attribute and Access Control

WatchGuard devices can use the **Group Attribute** value to set the attribute that carries the User Group information. This information is used for access control by certain VPN protocols.



If you are using multiple VPN protocols (such as SSL) then you may need to set the value to match their requirements.

7. 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	

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

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

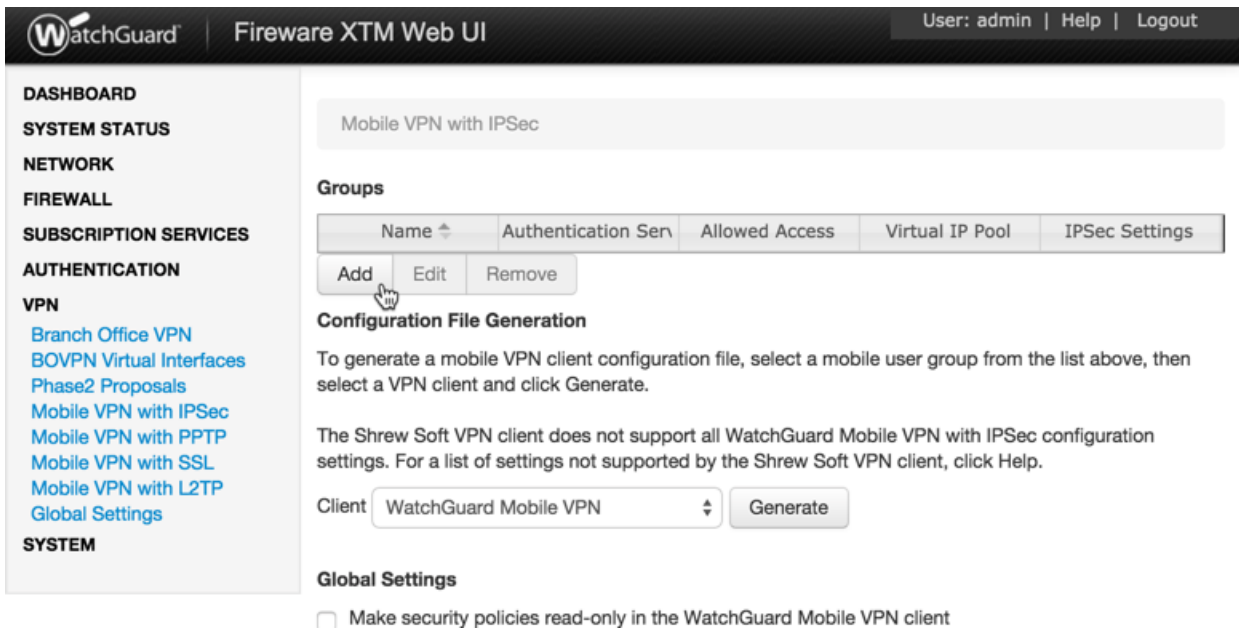
**DASHBOARD**  
**SYSTEM STATUS**  
**NETWORK**  
**FIREWALL**  
**SUBSCRIPTION SERVICES**  
**AUTHENTICATION**  
Branch Office VPN  
BOVPN Virtual Interfaces  
Phase2 Proposals  
Mobile VPN with IPsec  
Mobile VPN with PPTP  
Mobile VPN with SSL  
Mobile VPN with L2TP  
Global Settings  
**SYSTEM**

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

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



**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 IPSec

**Groups**

Name	Authentication Serv	Allowed Access	Virtual IP Pool	IPSec Settings
Add	Edit	Remove		

**Configuration File Generation**

To generate a mobile VPN client configuration file, select a mobile user group from the list above, then select a VPN client and click Generate.

The Shrew Soft VPN client does not support all WatchGuard Mobile VPN with IPSec configuration settings. For a list of settings not supported by the Shrew Soft VPN client, click Help.

Client WatchGuard Mobile VPN Generate

**Global Settings**

☐ Make security policies read-only in the WatchGuard Mobile VPN client

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

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 IPsec / Add

Name

General IPsec Tunnel Resources Advanced

**General Settings**

Authentication Server

**Passphrase**

Passphrase

Confirm

Firebox IP Addresses

Property	Explanation	Example
Name	A unique name for this group configuration. This name must match exactly the LDAP / AD group name configured in First Factor authentication Group Attribute (advanced).	Office VPN
Authentication Server	The type of device that users of this group will be authenticated with.	Radius
Passphrase	The secret shared between the Mobile VPN client and the RADIUS server. The secret must be provided to all IPsec users.	sharedsecret
Confirm	The secret shared between the Mobile VPN client and the RADIUS server.	sharedsecret
Primary	Primary IP address or domain name Firebox users connect to.	10.0.10.130
Backup (optional)	Secondary IP address or domain name Firebox users connect to.	10.0.10.131

### Mobile VPN with IPsec group profile name

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

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

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 IPsec / Add

Name: Office VPN

General IPsec Tunnel Resources Advanced

**General Settings**

Authentication Server: RADIUS

**Passphrase**

Passphrase: .....  
Confirm: .....

Firebox IP Addresses

12. Click **Save**

**Timeouts**

If the session and idle timeouts are configured on your authentication server, they will take precedence over these settings

Session Timeout: 480 minutes  
Idle Timeout: 30 minutes

Save Cancel

You are now ready to test your configuration.

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

## User Management

There are several options for managing your users within LoginTC:

- Individual users can be added manually in [LoginTC Admin Panel](#)
- Bulk operations using [CSV Import](#)

- Programmatically manage user lifecycle with the [REST API](#)
- One-way user synchronization of users to LoginTC Admin is performed using [User Sync Tool](#).

## Failover

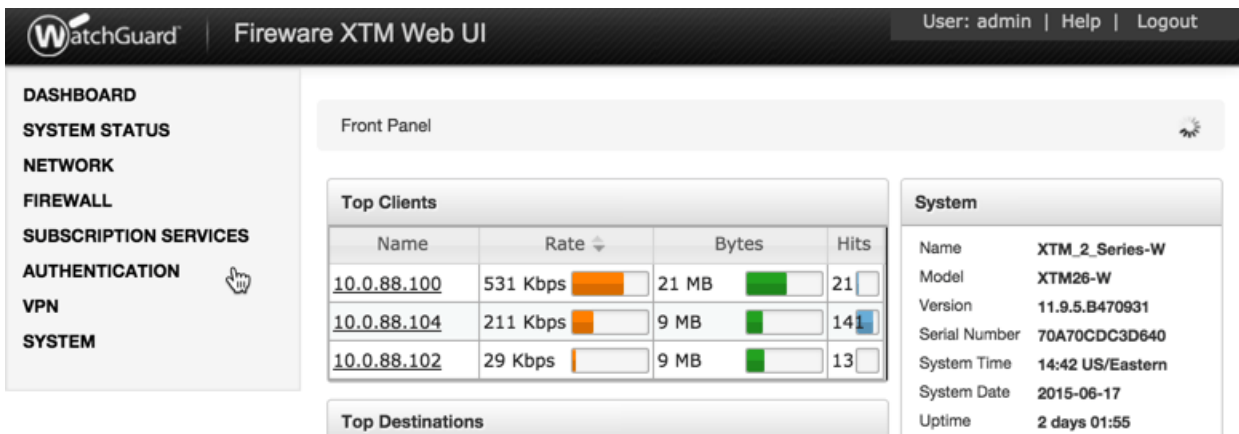
WatchGuard devices have built-in settings that make it easy to configure a secondary RADIUS server to provide failover.

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. The top navigation bar includes the WatchGuard logo, 'Fireware XTM Web UI', and user information 'User: admin | Help | Logout'. The left sidebar contains a list of navigation 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

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. The left sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION (with sub-items: Hotspot, Servers, Settings, Users and Groups, Web Server Certificate, Single Sign-On, Terminal Services, Authentication Portal), VPN, and SYSTEM. The 'Servers' link is highlighted. The main content area is titled 'Front Panel' and includes a refresh button. It displays two tables: 'Top Clients' and 'Top Destinations'. The 'System' section on the right shows details for the XTM\_2\_Series-W device, including its model, version, serial number, system time, date, uptime, and log server status. A 'Reboot' button and a time range selector (Last 20 Minutes) are also present.

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

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**

The screenshot shows the WatchGuard Fireware XTM Web UI 'Servers' page. The left sidebar is the same as in the previous screenshot, with 'Servers' highlighted. The main content area is titled 'Servers' and contains a section for 'Authentication Servers'. This section displays a table with columns for 'Server', 'Status', and 'Groups'. The 'RADIUS' server is highlighted with a mouse cursor.

Server	Status	Groups
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

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

## Logging

Logs can be found on the **Logs** tab:

The screenshot shows the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the text "LoginTC RADIUS Connector", and links for "Support" and "Log out". A left sidebar contains a menu with "GENERAL", "Endpoints", "User Directories", "Logs" (selected), "Status", "APPLIANCE", "Settings", "SETUP", "Settings", "Upgrade", and "Version 4.0.0". The main content area is titled "Logs" and displays a list of log entries for "authentication.log". The log entries show a sequence of events for user "john.doe", including "Simulating a RADIUS request", "Processing authentication", "Not performing password authentication", "Starting iframe authentication", and "Challenging user". Each entry includes a timestamp, a hex ID, and a log level (INFO or DEBUG).

## Troubleshooting

### User Receives Multiple LoginTC Requests

See the [Knowledge Base](#) articles:

### Authentication times out

See the [Knowledge Base](#) articles:

### 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 displays the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the text "LoginTC RADIUS Connector", and links for "Support" and "Log out". The left sidebar contains a menu with categories: GENERAL (with links to Endpoints, User Directories, Logs, and Status), APPLIANCE (with a link to Settings), and SETUP (with links to Settings and Upgrade). The main content area is titled "Status" and shows a green banner stating "All status checks have passed". Below this, three status checks are listed, each with a "Passed" result: "Connectivity to cloud.logintc.com", "CPU Usage", "RAM Usage", and "Disk Space". The bottom of the sidebar indicates the version is "Version 4.0.0".

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

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

Logs

authentication.log
Download
Refresh

```

2023-06-23T18:35:52.014Z [73e3aa80] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS
2023-06-23T18:35:52.020Z [73e3aa80] INFO Processing authentication for user john.doe in iframe authentication mode
2023-06-23T18:35:52.026Z [73e3aa80] DEBUG Not performing password authentication
2023-06-23T18:35:52.027Z [73e3aa80] DEBUG Starting iframe authentication
2023-06-23T18:35:52.167Z [73e3aa80] INFO Challenging user john.doe
2023-06-23T18:36:29.894Z [cb7036a0] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS
2023-06-23T18:36:29.895Z [cb7036a0] INFO Processing authentication for user john.doe in challenge interactive authentication mode
2023-06-23T18:36:29.898Z [cb7036a0] DEBUG Not performing password authentication
2023-06-23T18:36:30.034Z [cb7036a0] INFO Challenging user john.doe with primary challenge
2023-06-23T18:36:49.355Z [b17b1ac8] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS
2023-06-23T18:36:49.356Z [b17b1ac8] INFO Processing authentication for user john.doe in iframe authentication mode
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Not performing password authentication
2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Starting iframe authentication
2023-06-23T18:36:49.511Z [b17b1ac8] INFO Challenging user john.doe
2023-06-23T18:37:00.687Z [ab4d8546] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS
2023-06-23T18:37:00.687Z [ab4d8546] INFO Processing authentication for user john.doe in iframe

```

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](mailto: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
Refresh

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

51/61

Click on **Traffic Monitor**:

Name	Rate	Bytes	Hits
10.0.88.104	138 Kbps	11 MB	57
10.0.88.100	61 Kbps	873 KB	36
10.0.88.102	35 Kbps	10 MB	14

Name	Rate	Bytes	Hits
184.150.152.15	65 Kbps	1 MB	3
74.125.22.139	53 Kbps	2 MB	1
10.0.10.164	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

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

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\_prcs\_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 15:03:37 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: 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

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 endpoint you're having problems with:

The screenshot shows the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the text "LoginTC RADIUS Connector", and links for "Support" and "Log out". The left sidebar contains a menu with "GENERAL", "Endpoints", "User Directories", "Logs", "Status", "APPLIANCE", "Settings", "SETUP", "Settings", "Upgrade", and "Version 4.0.0". The main content area is titled "Endpoints" and features a "+ Create Endpoint" button. A yellow banner states: "Endpoints are application and network boundaries where users authenticate". Below this, a card for "Generic RADIUS (192.168.0.1)" is displayed, showing a shield icon and a list of associated endpoints: "Generic RADIUS", "Example Inc. Secure Access", and "AD (172.20.100.10)".

Scroll down to the **User Directory** section and next to **Group Attribute** click **Edit**:

The screenshot shows the configuration page for the "Generic RADIUS" endpoint. The top navigation bar is the same as the previous screenshot. The left sidebar is also the same. The main content area is titled "Endpoints / Generic RADIUS" and includes "Test Endpoint" and "Delete" buttons. Below the title, there is an "Edit" button. The "User Directory" section shows a table with two rows: "User Directory" with the value "AD (172.20.100.10)" and an "Edit" button, and "Group Attribute" with the value "None" and an "Edit" button. The "Challenge Strategy" section shows a table with one row: "Challenge Strategy" with the value "Challenge all users" and an "Edit" button. The "Client Settings" section is partially visible at the bottom.

1. If “None” is selected, change it to “Specify a group attribute”. [Click here](#) to review how to configure the Group Attribute for SSL

The screenshot shows the 'Group Attribute' configuration page in the LoginTC RADIUS Connector. The left sidebar contains a navigation menu with 'Endpoints' selected. The main content area has the title 'Group Attribute' and two radio buttons: 'None' (selected) and 'Specify a Group attribute'. Below the radio buttons, there is a text field for 'Specify an additional user group attribute to be returned to the authentication server.' and a note: 'Do not send additional Group Attribute information.' A green 'Save' button is located at the bottom right of the main content area. The top navigation bar includes the LoginTC logo, 'LoginTC RADIUS Connector', and links for 'Support' and 'Log out'.

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.

The screenshot shows the 'Group Attribute' configuration page in the LoginTC RADIUS Connector. The left sidebar contains a navigation menu with 'Endpoints' selected. The main content area has the title 'Group Attribute' and two radio buttons: 'None' and 'Specify a Group attribute' (selected). Below the radio buttons, there is a text field for 'Specify an additional user group attribute to be returned to the authentication server.' and a section titled 'RADIUS Group Attribute' with a text input field labeled 'Filter-Id'. Below this, there is a section titled 'Groups' with a text input field containing 'SSLVPN-Users'. A note explains that the user must be a member of a group for the attribute to be sent back. At the bottom, there are 'Test' and 'Save' buttons, and a yellow box with the text 'Click Test before continuing.'

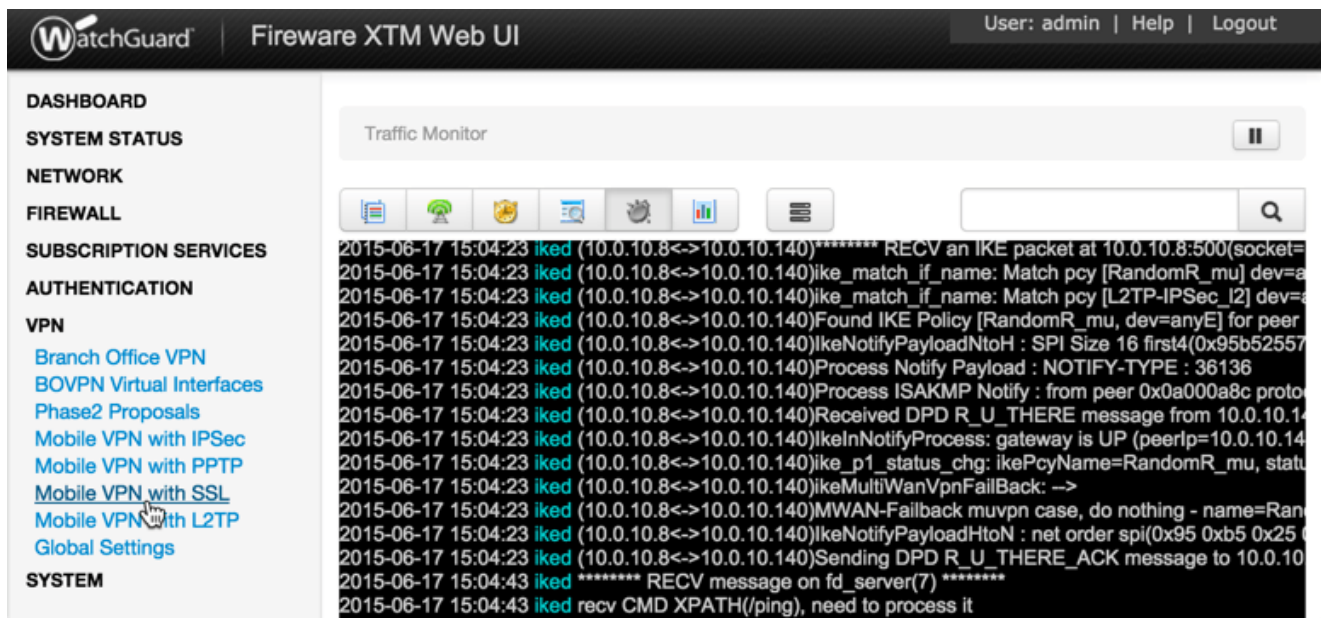
If you find a log message similar to this:



```
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
```

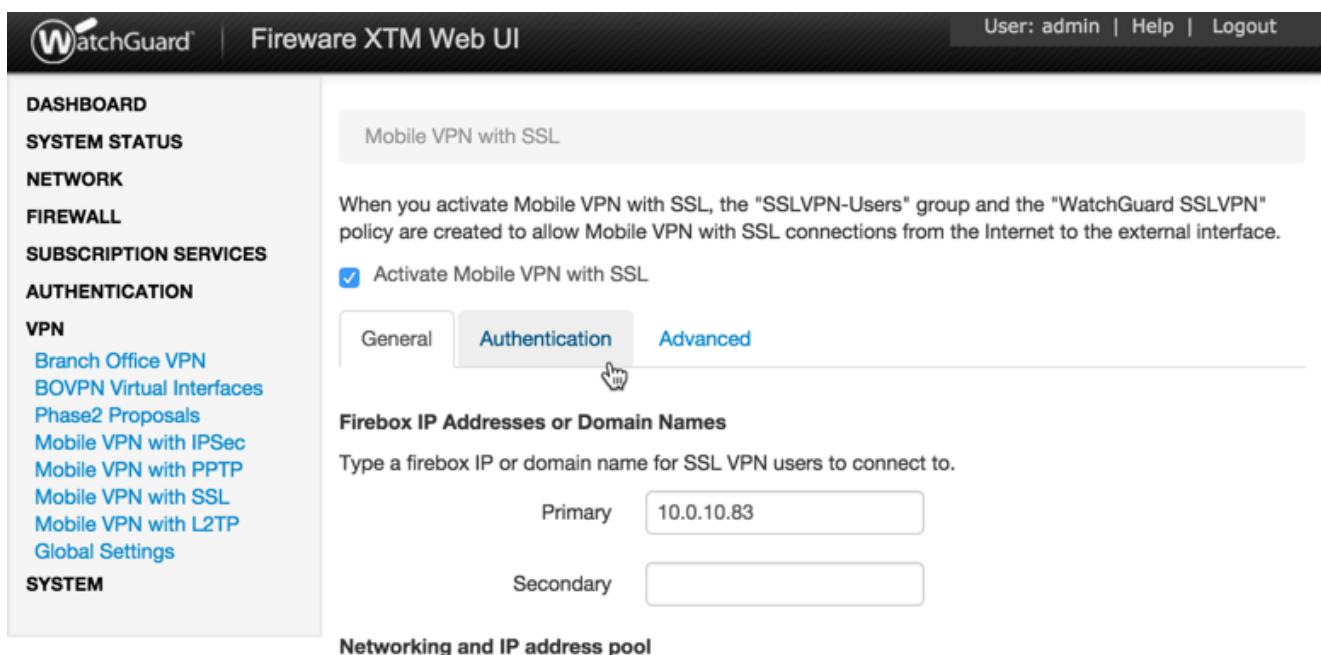
Then the RADIUS server is sending back a Group Attribute, but it may not be the correct one.

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** :



The screenshot shows the WatchGuard Fireware XTM Web UI. The left-hand navigation bar is expanded, showing the following menu items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, and VPN. Under the VPN section, the following options are listed: Branch Office VPN, BOVPN Virtual Interfaces, Phase2 Proposals, Mobile VPN with IPsec, Mobile VPN with PPTP, Mobile VPN with SSL (highlighted with a mouse cursor), Mobile VPN with L2TP, and Global Settings. The main content area displays the Traffic Monitor log, which shows a series of IKE-related messages between 10.0.10.8 and 10.0.10.140. The messages include IKE packet reception, IKE match if name, IKE policy found, IKE notify payload, and IKE status changes.

Click on the **Authentication** tab:



The screenshot shows the WatchGuard Fireware XTM Web UI configuration page for Mobile VPN with SSL. The left-hand navigation bar is expanded, showing the following menu items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, and VPN. Under the VPN section, the following options are listed: Branch Office VPN, BOVPN Virtual Interfaces, Phase2 Proposals, Mobile VPN with IPsec, Mobile VPN with PPTP, Mobile VPN with SSL (highlighted with a mouse cursor), Mobile VPN with L2TP, and Global Settings. The main content area displays the configuration for Mobile VPN with SSL. The page title is "Mobile VPN with SSL". Below the title, there is 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 the description, there is a checkbox labeled "Activate Mobile VPN with SSL" which is checked. Below the checkbox, there are three tabs: General, Authentication (highlighted with a mouse cursor), and Advanced. Below the tabs, there is a section titled "Firebox IP Addresses or Domain Names" with the instruction "Type a firebox IP or domain name for SSL VPN users to connect to." Below this instruction, there are two input fields: "Primary" with the value "10.0.10.83" and "Secondary" which is empty. Below the input fields, there is a section titled "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

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

## 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**



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="#">10.0.88.100</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

Top Destinations

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**

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
<a href="#">10.0.88.100</a>	151 Kbps	3 MB	22
<a href="#">10.0.88.104</a>	105 Kbps	8 MB	118
<a href="#">10.0.88.102</a>	28 Kbps	9 MB	14

Top Destinations

Name	Rate	Bytes	Hits
<a href="#">184.150.152.14</a>	126 Kbps	2 MB	1
<a href="#">74.125.29.101</a>	20 Kbps	646 KB	1
<a href="#">136.146.210.32</a>	19 Kbps	177 KB	2
<a href="#">184.150.152.18</a>	18 Kbps	137 KB	2

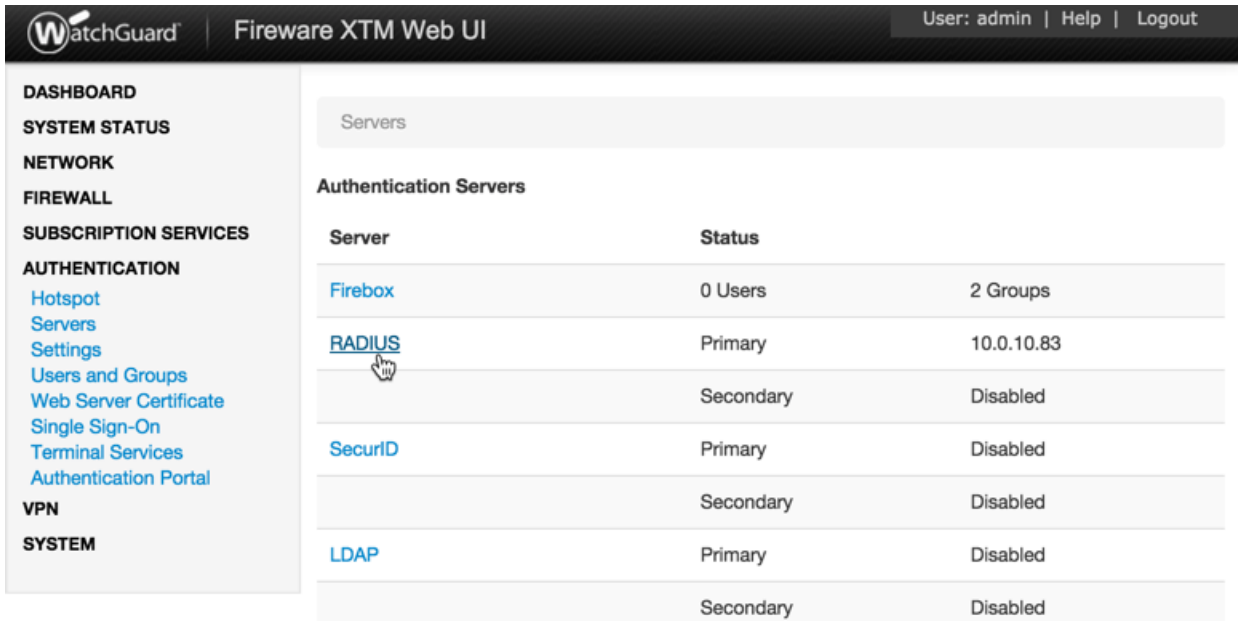
System

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

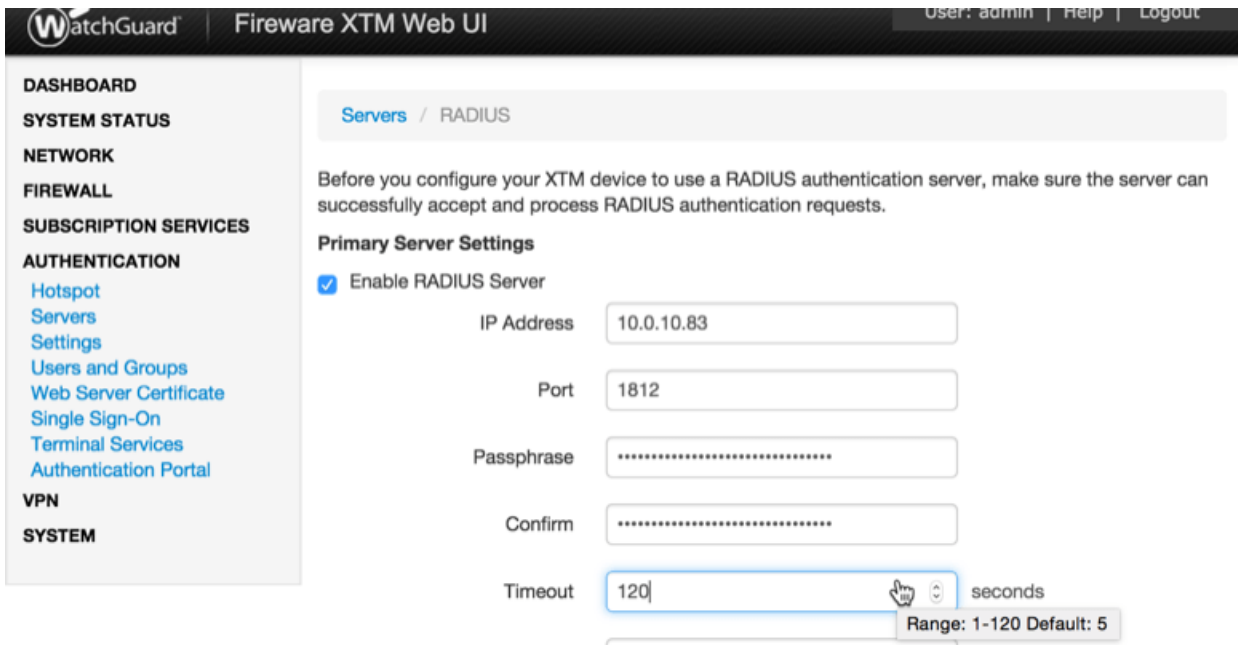
## 2. Click **RADIUS**



The screenshot shows the WatchGuard Fireware XTM Web UI. The left sidebar contains a navigation menu with categories: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. Under AUTHENTICATION, there are links for Hotspot, Servers, Settings, Users and Groups, Web Server Certificate, Single Sign-On, Terminal Services, and Authentication Portal. The main content area is titled 'Authentication Servers' and displays a table with columns 'Server' and 'Status'.

Server	Status
Firebox	0 Users 2 Groups
<b>RADIUS</b>	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.



The screenshot shows the WatchGuard Fireware XTM Web UI with the 'RADIUS' configuration page selected. The page title is 'Servers / RADIUS'. Below the title, there is a note: 'Before you configure your XTM device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.' The 'Primary Server Settings' section includes a checkbox 'Enable RADIUS Server' which is checked. Below this are input fields for 'IP Address' (10.0.10.83), 'Port' (1812), 'Passphrase', and 'Confirm'. The 'Timeout' field is set to 120 seconds, with a tooltip indicating 'Range: 1-120 Default: 5'.

See the [Knowledge Base](#) articles for more information:

### Email Support

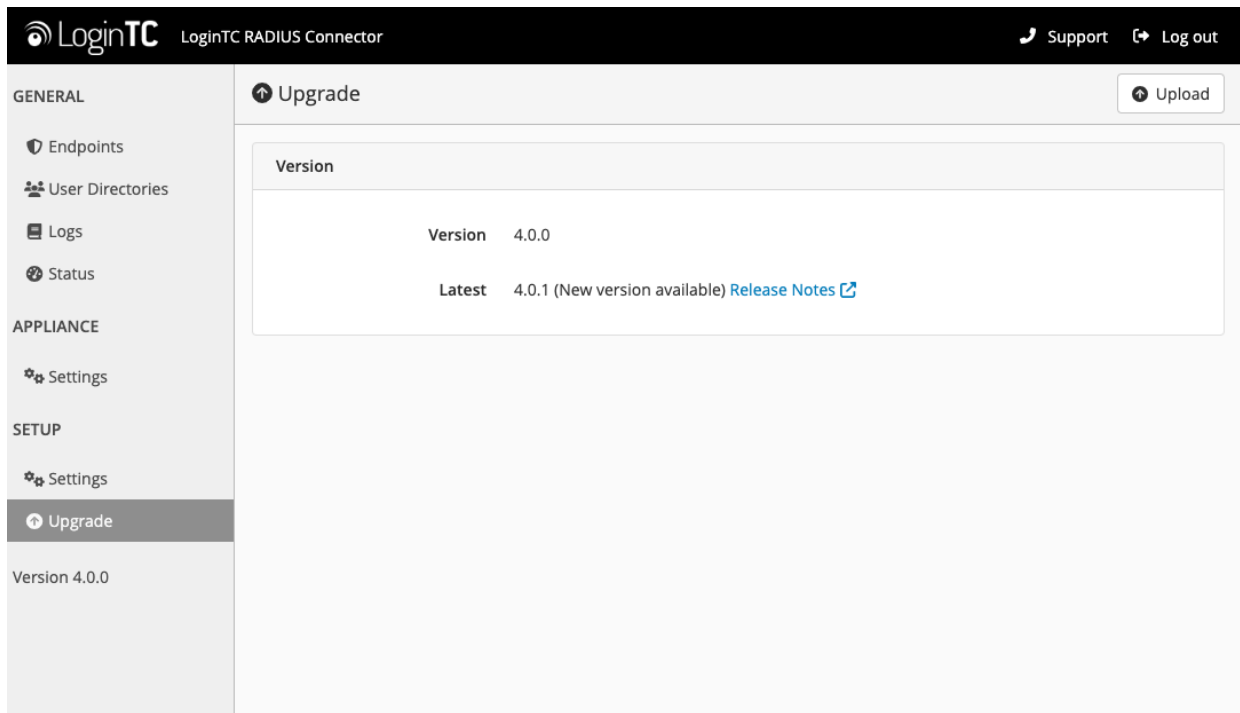
For any additional help please email [support@cyphercor.com](mailto:support@cyphercor.com). Expect a speedy reply.

### Upgrading

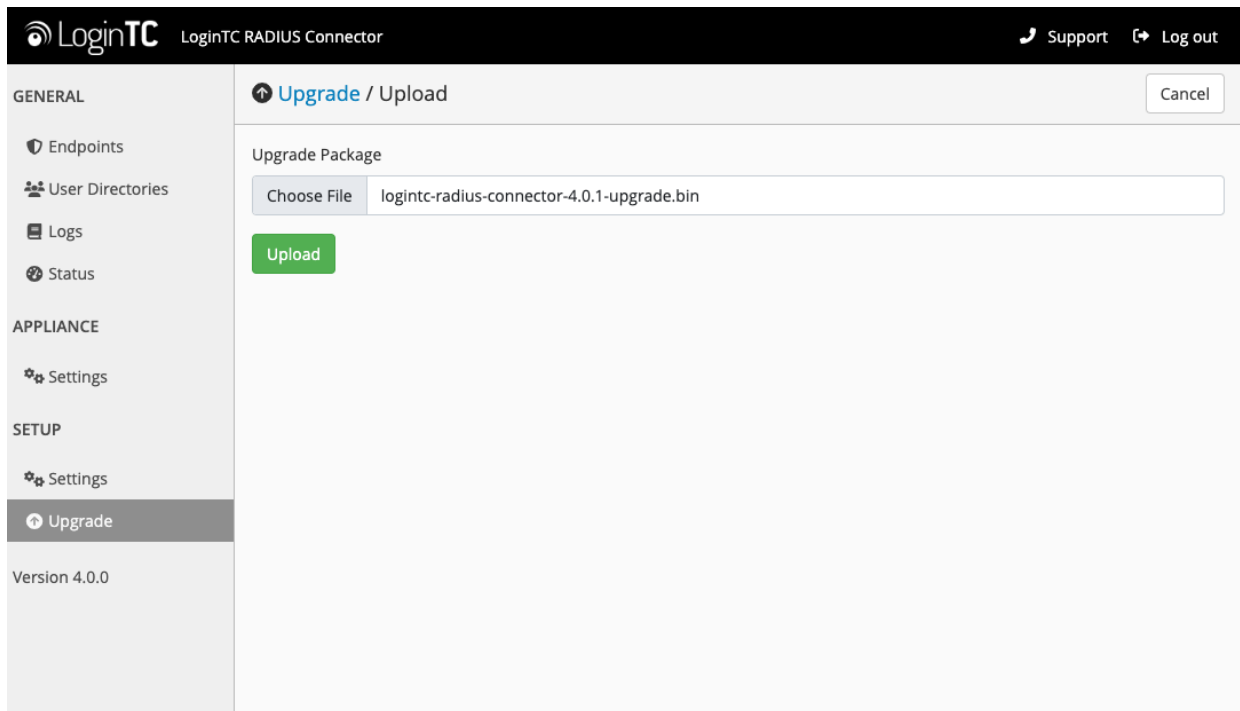
### From 4.X

The latest LoginTC RADIUS Connector upgrade package can be downloaded here:  
[Download RADIUS Connector \(Upgrade\)](#).

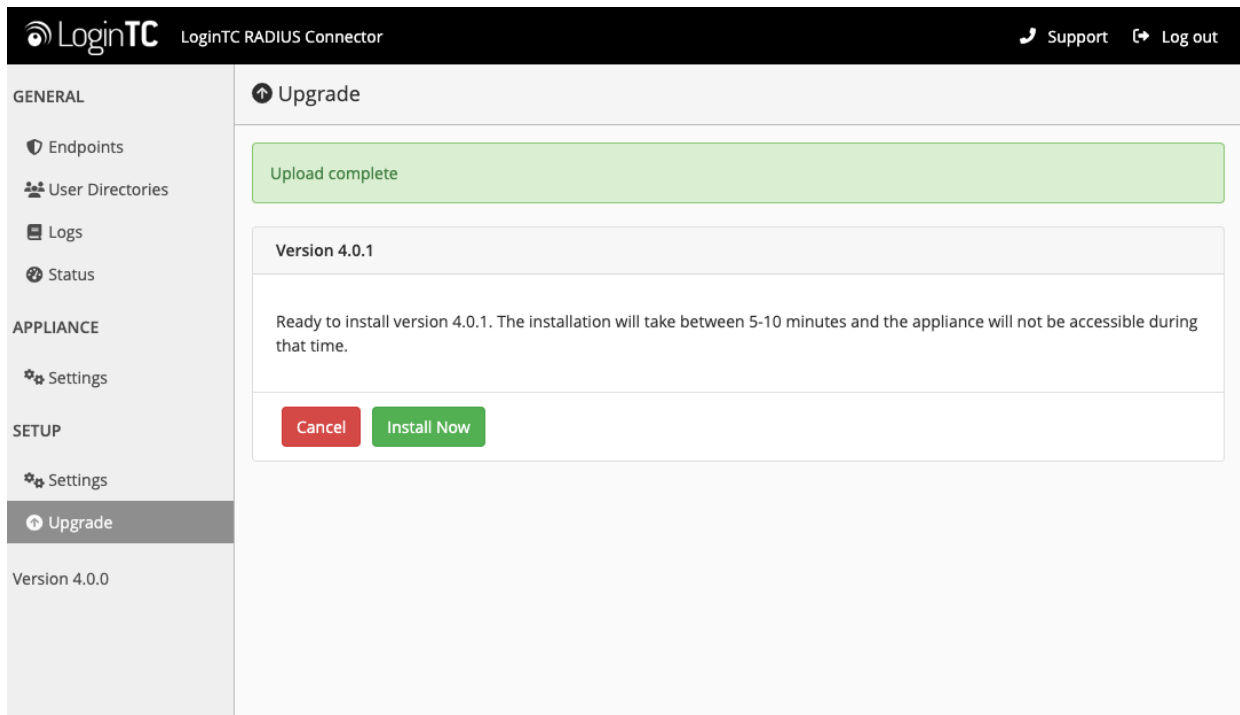
1. Navigate to **SETUP > Upgrade**:



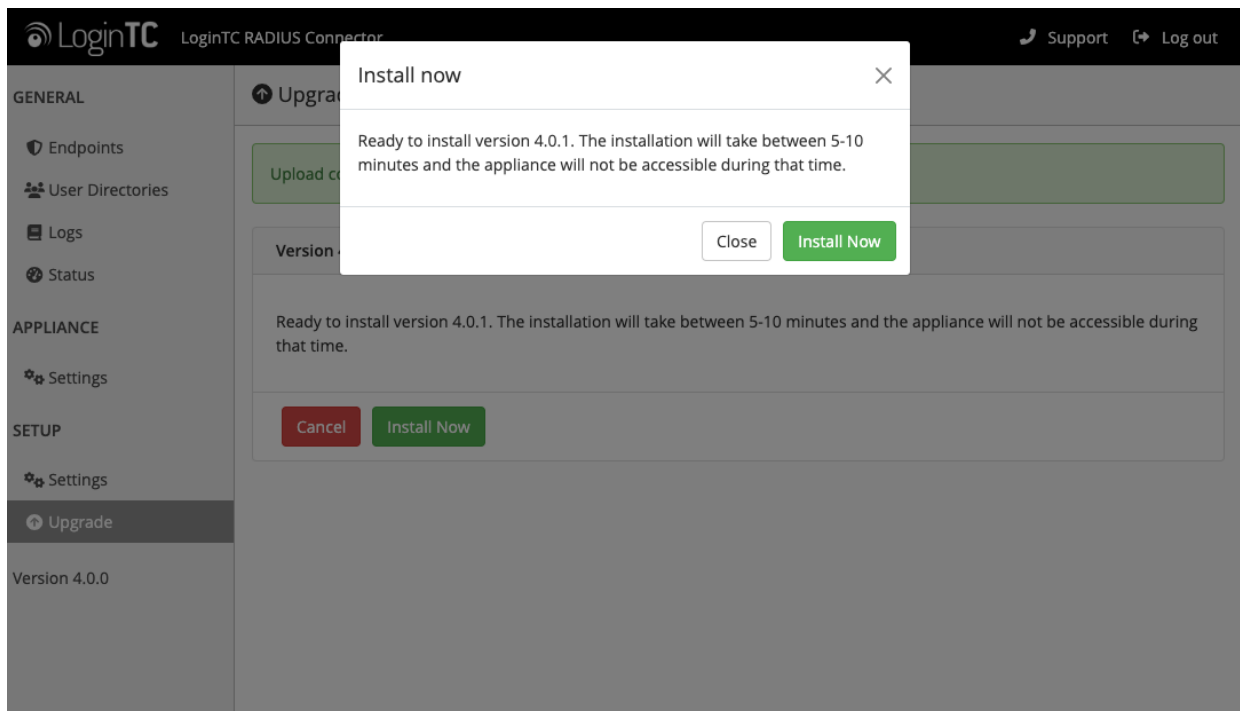
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



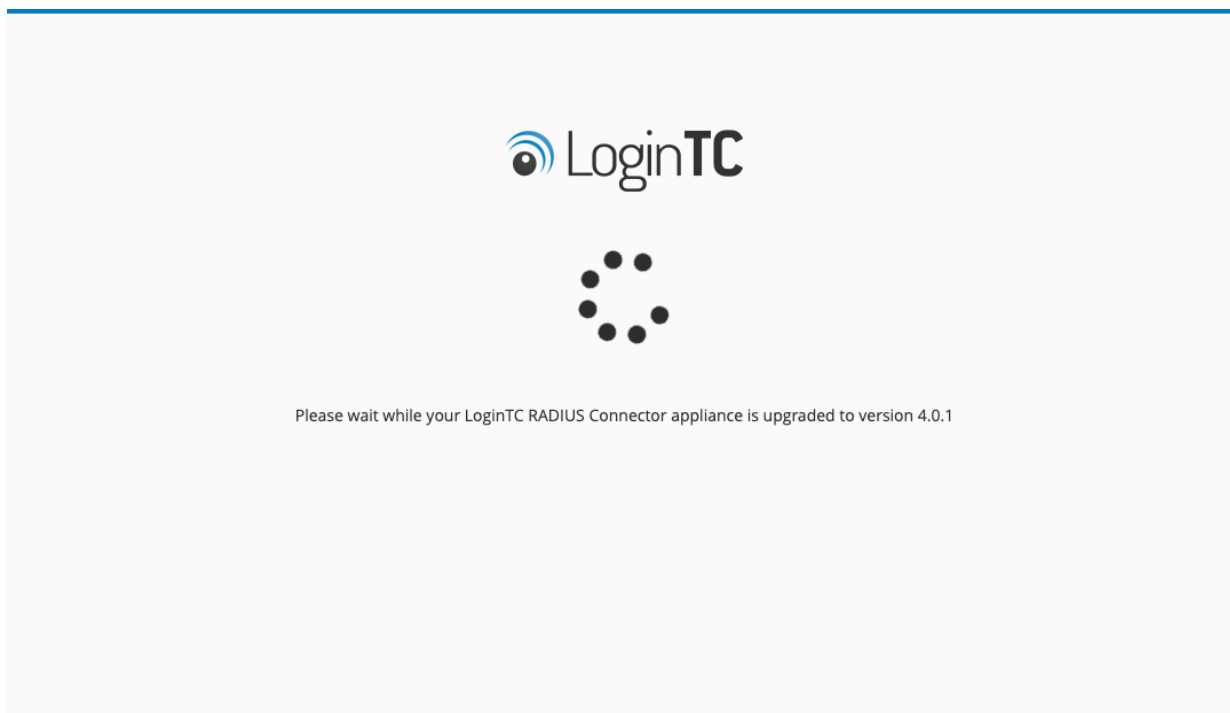
3. Click **Upload** and do not navigate away from the page:



4. Once upload is complete upgrade by clicking **Install Now**:



5. Wait 10-15 minutes for upgrade to complete:



**NOTE: Upgrade time**

Upgrade can take 10-15 minutes, please be patient.

**From 3.X**

**Important: LoginTC RADIUS Connector 3.X End-of-life**

The LoginTC RADIUS Connector 3.X virtual appliance is built with CentOS 7.9. CentOS 7.X is End of Lifetime (EOL) June 30th, 2024. See [CentOS Product Specifications](#). Although the appliance will still function it will no longer receive updates and nor will it be officially supported.

**New LoginTC RADIUS Connector 4.X**

A new LoginTC RADIUS Connector 4.X virtual appliance has been created. The Operating System will be supported for many years. Inline upgrade is not supported. As a result upgrade is deploying a new appliance. The appliance has been significantly revamped and although the underlying functionality is identical, it has many new features to take advantage of.

Complete 3.X to 4.X upgrade guide: [LoginTC RADIUS Connector Upgrade Guide](#)