# Two factor authentication for WatchGuard XTM and Firebox IPSec Alternative

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

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

#### **User Experience**

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

## Architecture / Compatibility



# Compatibility

WatchGuard appliance compatibility:

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

#### Appliance not listed?

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

#### **Compatibility Guide**

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

#### Prerequisites

Before proceeding, please ensure you have the following:

## **RADIUS Domain Creation**

If you have already created a LoginTC domain for your LoginTC RADIUS Connector, then you may skip this section and proceed to <u>Installation</u>.

- 1. Log in to LoginTC Admin
- 2. Click Domains:
- 3. Click Add Domain:

ခါ Login <b>TC</b> ေ	ample Inc. 🧧 Docs 🔍 Support 🔺 administrator@example.com 🗸
GENERAL	+ Create
🆀 Dashboard	
🚓 Domains	A domain represents a service, e.g. VPN or website that you want to protect. It contains a collection of users and token policies.
🖀 Users	
🗐 Logs	
SETUP	
Administrators	
📽 Settings	You haven't created any domains yet.
	+ Create your first domain

4. Enter domain information:



#### Name

Choose a name to identify your LoginTC domain to you and your users

# Connector

RADIUS

#### Installation

The LoginTC RADIUS Connector runs <u>CentOS</u> 6.8 with <u>SELinux</u>. A firewall runs with the following open ports:

Port	Protocol	Purpose
22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
443	TCP	Web interface
80	TCP	Web interface
80	TCP	Package updates (outgoing)

Port	Protocol	Purpose

123 UDP NTP, Clock synchronization (outgoing)

#### Note: Username and Password

**logintc-user** is used for SSH and web access. The default password is **logintcradius**. You will be asked to change the default password on first boot of the appliance and will not be able to access the **web interface** unless it is change.

The logintc-user has sudo privileges.

# Configuration

Configuration describes how the appliance will authenticate your <u>RADIUS</u>-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<u>LoginTC Admin</u> 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 <u>RADIUS</u>-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.

٥L	ogin <b>TC</b>	Login	TC RADIUS Connector 2.1.0	E	Docs	📞 Support	占 log	gintc-user <del>-</del>
GENERA	۸L		🚠 Configurations		R	estart RADIUS Se	rver	+ Create
🚠 Co	nfigurations			-	_			
🗐 Log	gs							
APPLIAN	NCE							
🚯 Sta	atus		You	haven't created any configurations ye	et.			
🕸 Set	ttings							
🗐 Up	grade			+ Create your first configuration				

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

# LoginTC Settings

Configure which LoginTC organization and domain to use:

ခါ Login <b>TC</b> Login	TC RADIUS Connector 2.4.0	🗐 Docs 🥾 Support 🛔 logintc-user 🗸
GENERAL	Configurations /	New Configuration / LoginTC Settings Step 1 of 4 Cancel
📥 Configurations	LoginTC Settings	API Key
Logs	Values which will dictate how	
APPLIANCE	Connector will identify itself to the LoginTC cloud service.	The 64-character organization API key is found on the LoginTC Admin Panel Settings page.
🚯 Status	5	Domain ID
📽 Settings		The 40-character domain ID is found on the LoginTC Admin Panel domain settings page.
┛ Upgrade		Request Timeout
		60
		The amount of time the LoginTC RADIUS Connector should poll for a user to respond. This 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.

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 <u>Settings</u> 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:

ခာ Login <b>TC</b> ၊ ဖ	inTC RADIUS Connector 2.1.0	🗐 Docs 💪 Support 🔺 logintc-user 🗸
GENERAL	🚠 New Configuration	The settings Step 1 of 4 Cancel
A Configurations	LoginTC Settings	API Key
🖻 Logs	Values which will dictate how	vZkDw7l6Z3tApwZJXERseKdR0s5RNNqjMxXlwvxpWwJOa9oJXi9b5tdvPyFsqzwJ
APPLIANCE	will identify itself to the LoginTC cloud service.	The 64-character organization API key is found on the LoginTC Admin Panel Settings page.
🚳 Status		Domain ID
₫ <sup>®</sup> Settings		9120580e94f134cb7c9f27cd1e43dbc82980e152
- Settings		The 40-character domain ID is found on the LoginTC Admin Panel domain settings page.
┛ Upgrade		
		A Test Next
		Test successful, click Next to continue

## First Authentication Factor

Configure the first authentication factor to be used in conjunction with LoginTC. You may use Active Directory / LDAP or an existing RADIUS server. You may also opt not to use a first factor, in which case LoginTC will be the only authentication factor.

ခာ Login <b>TC</b> ဖ	inTC RADIUS Connector 2.1.0	🖻 Docs 🕓 Support 🔺 logintc-user 🗸
GENERAL	📥 New Configuratio	n / First Factor Step 2 of 4 Cancel
Configurations  Logs	First Factor Select the first way users will authenticate prior to LoginTC.	• LDAP Active Directory RADIUS None Connect to an existing LDAP server for username / password verification.
<ul> <li>Status</li> <li>Settings</li> <li>Upgrade</li> </ul>	LDAP Server Details The LDAP host and port information.	Host Host Host name or IP address of the LDAP server. Examples: Idap.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**:

ခာ Login <b>TC</b> မ	oginTC RADIUS Connector 2.1.0	🖻 Docs 🥾 Support 🛔 logintc-user 🗸
GENERAL	📥 New Configuratio	n / First Factor Step 2 of 4 Cancel
Configurations  Logs	First Factor Select the first way users will authenticate prior to LoginTC.	○ LDAP          • Active Directory ○ RADIUS ○ None Connect to an existing Active Directory server for username / password verification.
APPLIANCE  Status  Settings  Upgrade	AD Server Details The Active Directory host and port information.	Host 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	<pre>cn=admin,dc=example,dc=com</pre>
bind_password	The password for the above bind_dn account	password
base_dn	The top-level DN that you wish to query from	<pre>dc=example,dc=com</pre>

Property	Explanation	Examples
attr_username	The attribute containing the user's username	sAMAccountName or uid
attr_name	The attribute containing the user's real name	displayName or cn
attr_email	The attribute containing the user's email address	mail or email
Group Attribute (optional)	Specify an additional user group attribute to be returned the authenticating server.	Office VPN
RADIUS Group Attribute (optional)	Name of RADIUS attribute to send back	Filter-Id
LDAP Group / AD Group (optional)	A comma delimited list of the names of possible LDAP groups to be sent back to the authenticating server. The user must be a member of a group for the attribute to be sent back. Groups membership is checked in priority order, if the user is a member of multiple groups the first group matched is returned.	Office VPN or Administrators,Sales,Engineers
encryption (optional)	Encryption mechanism	ssl or startTLS
cacert (optional)	CA certificate file (PEM format)	/opt/logintc/cacert.pem

## Group Attribute and Access Control

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

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

ි Login <b>TC</b>	Login	TC RADIUS Connector 2.1.0	🖻 Docs 🔍 Support 🚢 logint	tc-user <del>-</del>
GENERAL		📥 New Configuration	on / First Factor Step 2 of 4	Cancel
Configurations				
Logs		Group Attribute (Advanced)	None      Specify a Group Attribute	
APPLIANCE		Specify an additional user	RADIOS Group Attribute	
Status		group attribute to be returned	Filter-Id	
🌣 Settings		the authenticating server.	Name of RADIUS attribute to send back. For example, for WatchGuard this is the named the Group Attribute, e.g. for a Group Attribute value of 11, use: Filter-Id.	value of
┛ Upgrade			LDAP Group	
			The name of the LDAP group to be sent back to the authenticating server. The user must member of the group for the attribute to be sent back. of Examples: SSLVPN-Users.	t be a
		C		

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:

ک Login <b>TC</b> دمونہ	TC RADIUS Connector 2.1.0	🖻 Docs 🕓 Support 🔮 logintc-user 🗸
GENERAL	🚓 New Configuration	n / First Factor Step 2 of 4 Cancel
🛔 Configurations	First Factor	○ LDAP ○ Active Directory ● RADIUS ○ None
🗐 Logs	Select the first way users will authenticate prior to LoginTC.	Connect to an existing RADIUS server for username / password verification.
APPLIANCE		
🙆 Status	RADIUS Server	Host
Settings	The RADIUS host and secret.	Host name or IP address of the RADIUS server. Examples: ldap.example.com or 192.168.1.42
🗐 Upgrade		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 <b>or</b> 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 <u>Static List</u> option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured <u>First Authentication Factor</u>. 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 <u>Active Directory or LDAP Group</u> 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 <u>First Authentication Factor</u>.

#### No Passthrough (default)

ම Login <b>TC</b> 🛛	ginTC RADIUS Connector 2.1.0		Docs	Support	💄 logintc-user 🗸
GENERAL	🚠 New Configuratio	on / Passthrough		Step	3 of 4 Cancel
Left Configurations	Passthrough	● No Passthrough 🔘 Static List 🔘 LDAP Grou	up 🔾 Acti	ve Directory Gro	pup
🖉 Logs	Configure list of users which will not be challenged by	All authentications will be challenged with LoginTC	. This can b	e configured at a	anytime.
APPLIANCE	LoginTC.				
Status		Next			
🕸 Settings					
┛ Upgrade					

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

#### Static List

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

ه Login <b>TC</b>	oginTC RADIUS Connector 2.1.0	🖻 Docs	Support ▲ logintc-user +
GENERAL	🛔 New Configuration	n / Passthrough	Step 3 of 4 Cancel
<ul><li>Configurations</li><li>Logs</li></ul>	Passthrough Configure list of users which will not be challenged by	○ No Passthrough ③ Static List ○ LDAP Group ○ Active Store static list of users that will be challenged with LoginTC. Go	e <b>Directory Group</b> ood for small number of users.
APPLIANCE	LoginTC.		
<ul> <li></li></ul>	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	
			le le

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.

ခါ Login <b>TC</b> ၊ ဖ	nTC RADIUS Connector 2.1.0	🗐 Docs 🕓 Support 🔒 logintc-user 🗸
GENERAL	🛔 New Configuration	A / Passthrough Step 3 of 4 Cancel
🛔 Configurations	Passthrough	○ No Passthrough ○ Static List ○ LDAP Group ④ Active Directory Group
🗐 Logs	Configure list of users which will not be challenged by	Connect to an existing Active Directory server for group membership verification. Good for large number of users.
APPLIANCE	LoginTC.	
🚯 Status	Auth Groups	LoginTC challenge Auth Groups
🕸 Settings	Only users which are members	
Upgrade	or one or more or the specified groups will be challenged with LoginTC. All other users will be challenged with configured first factor only.	Comma separated list of groups membership for which users will be challenged with LoginTC. Example: logintc_users, operations
	AD Server Details	Host
	The Active Directory host and port information.	

### Configuration values:

Property	Explanation	Examples
LoginTC challenge auth groups	Comma separated list of groups for which users will be challenged with LoginTC	Office VPN or two-factor- users
host	Host or IP address of the LDAP server	ldap.example.com or 192.168.1.42
port (optional)	Port if LDAP server uses non-standard (i.e., 389 / 636 )	4000
bind_dn	DN of a user with read access to the directory	<pre>cn=admin,dc=example,dc=com</pre>
<pre>bind_password</pre>	The password for the above bind_dn account	password
base_dn	The top-level DN that you wish to query from	<pre>dc=example,dc=com</pre>
attr_username	The attribute containing the user's username	sAMAccountName or uid
attr_name	The attribute containing the user's real name	displayName or cn
attr_email	The attribute containing the user's email address	mail or email

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

#### Configuration Simplified

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

Click Test to validate the values and then click Next.

#### Client and Encryption

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



#### Client configuration values:

Property	Explanation	Examples
name	A unique identifier of your RADIUS client	CorporateVPN
ip	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	192.168.1.44
secret	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret

Under Authentication Mode select Direct

ම Login <b>TC</b>	LoginTC RADIUS Connector 2.5.1	🔊 Docs 🕓 Support 🔺 logintc-user 🗸
GENERAL	🚠 Configurations /	New Configuration / Client and Encryption Step 4 of 4 Cancel
Configurations Logs APPLIANCE		Secret The secret shared between your RADIUS client and the LoginTC RADIUS Connector.
<ul><li>֎ Status</li><li>✿ Settings</li></ul>	Authentication Mode How the LoginTC RADIUS Connector will perform the second factor.	● Direct
	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 LoginTC RADIUS Connector will directly and automatically perform the LoginTC second factor. See <u>User Experience</u> for more information.

# Data Encryption

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

Click Test to validate the values and then click Save.



# Testing (Connector)

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

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



## Click Test Configuration:

ခါ Login <b>TC</b> ဖေး	inTC RADI <u>US Connector 2.1.0 📓 Docs</u> 💺 Support 🛔 logintc-	user <del>-</del>
GENERAL	Test Configuration	Treate
Configurations     Logs     APPLIANCE	Test the first and second factor authentication by simulating an actual RADIUS request. The resulting test LoginTC request will look identical to what a user would receive in a real authentication scenario. If the authenticating user is configured to passthrough then only the first factor challenge will apply.	tion
<ul> <li>Status</li> <li>Settings</li> </ul>		
🧧 Upgrade	Username Enter username	
	Password Password	
	For LoginTC only authentication leave Password field blank.	
	Close 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:

ခါ Login <b>TC</b> ဖ	ginTC RADIUS Connector 2.1.0 🖉 Docs 🕓 Support 👗 logintc-user 🗸
GENERAL	Logs
🛔 Configurations	
🗐 Logs	/var/log/logintc/authenticate.log /var/log/radius/radius.log /var/log/logintc/tornado.log
APPLIANCE	<pre>V=+.0.5 (10.0.10.176) 1.15MS 2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms 2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms 2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms 2015-04-28 17:10:21,624 - INFO - 304 GET / (10.0.10.178) 2.43ms 2015-04-28 17:10:21,624 - INFO - 304 GET /configurations (10.0.10.178) 2.45ms 2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms 2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms 2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms 2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms 2015-04-28 17:10:22,102 - 10FO - 304 GET /logs (10.0.10.178) 3.00ms</pre>
	Displaying last 1000 lines, refreshes automatically every 1 second.

# 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:

ම Login <b>TC</b>	Login	TC RADIUS Connector 2.1.0			Docs	Support	💄 logintc-user <del>-</del>
GENERAL		📽 Settings					
📥 Configurations							
🗐 Logs		Appliance					
APPLIANCE		IP Address	10.0.10.116				
Status		RADIUS Authentication	1812				
🕫 Settings		Tore					
🖉 Upgrade		RADIUS Accounting Port	1813				

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)

WatchGuard Fireware >	(TM Web UI
	Usemame admin Password 

2. Click Authentication:

WatchGuard Firewa	re XTM Web UI				User: admin   Help   Logout
DASHBOARD Front Panel Subscription Services	Front Panel				C
Interfaces	Top Clients				System
Gateway Wireless Controller	Name	Rate 🜩	Bytes	Hits	Name XTMv
SYSTEM STATUS	10.0.1.5	150 Kbps	341 KB	17	Model XTMv
NETWORK	10.0.10.178	13 Kbps	1 KB	1	Version 11.8.B432340 Serial Number V1C5000000000
FIREWALL	Ten Destination	_			System Time 12:48 US/Eastern
SUBSCRIPTION SERVICES	Top Destination	s			System Date 2013-12-13
AUTHENTICATION	Name	Rate 😓	Bytes	Hits	Uptime 0 days 00:14
VPN	23.60.247.88	109 Kbps	142 KB	6	Log Server Disabled
SYSTEM	173.194.43.111	19 Kbps 🚪	113 КВ 📕	1	Reboot
	10.0.10.183	13 Kbps	1 KB	1	
	23.61.177.207	7 Kbps	9 КВ	1	
	184.150.152.18	6 Kbps	52 KB	2	Last 20 Minutes
	63.140.54.90	3 Kbps	3 КВ	1	External Bandwidth

3. Under Authentication click Servers:

WatchGuard Firewa	re XTM Web UI				User: admin   Help   Logout
DASHBOARD Front Panel Subscription Services FireWatch Interfaces	Front Panel				System
Traffic Monitor	Name	Rate 🗘	Bytes	Hits	Name XTMv
SYSTEM STATUS	10.0.10.178	13 Kbps	1 KB	1	Model XTMv
NETWORK	10.0.1.5	4 Kbps	58 КВ	3	Version 11.8.B432340
FIREWALL SUBSCRIPTION SERVICES	Top Destination	s			System Time 12:50 US/Eastern System Date 2013-12-13
AUTHENTICATION	Name	Rate 🗘	Bytes	Hits	Uptime 0 days 00:16
Hotspot	10.0.10.183	13 Kbps	1 KB	1	Log Server Disabled
<u>Settings</u>	184.150.152.18	2 Kbps 📕	48 KB	1	Reboot
Users and Groups	66.196.113.5	1 Kbps	4 КВ	1	
Single Sign-On Terminal Services	173.192.82.194	208 bps	6 КВ	1	Last 20 Minutes 🛊
VPN	Top Policies				
SYSTEM	Name	Rate 🚖	Bytes	Hits	External Bandwidth

4. Under Authentication Servers click RADIUS:

WatchGuard Firewa	re XTM Web UI	l	Jser: admin   Help   Logout
DASHBOARD SYSTEM STATUS	Servers		
NETWORK	Authentication Servers		
SUBSCRIPTION SERVICES	Server	Status	
AUTHENTICATION Hotspot	Firebox	0 Users	0 Groups
Servers Settings	RADIUS	Primary	Disabled
Users and Groups Web Server Certificate	-	Secondary	Disabled
Single Sign-On Terminal Services VPN SYSTEM	SecurID	Primary	Disabled
		Secondary	Disabled
	LDAP	Primary	Disabled
		Secondary	Disabled
	Active Directory	0 domains	

5. Under Primary Server Settings click Enable RADIUS Server:

WatchGuard Firewa	are XTM Web UI		User: admin   Help   Logout
DASHBOARD SYSTEM STATUS	Servers / RADIUS		
NETWORK FIREWALL SUBSCRIPTION SERVICES	Before you configure your XTM d successfully accept and process	levice to use a RADIUS authenticat RADIUS authenticats.	ion server, make sure the server can
AUTHENTICATION Hotspot Servers	Enable RADIUS Server		
Users and Groups Web Server Certificate Single Sign-On	Port	1812	٢
Terminal Services	Passphrase		
SYSTEM	Confirm		
	Timeout	5	(t) seconds
×.	Retries	3	٢

6. Complete Primary Server Settings form:

FIREWALL	successfully accept and process	RADIUS authentication requests.	
SUBSCRIPTION SERVICES	Primary Server Settings		
AUTHENTICATION Hotspot Servers Settings	<ul> <li>Enable RADIUS Server</li> </ul>		_
	IP Address	10.0.10.130 I	
Users and Groups Web Server Certificate Single Sign-On	Port	1812	٢
Terminal Services	Passphrase	•••••	
SYSTEM	Confirm	•••••	
	Timeout	60	(;) seconds
	Retries	1	٢
	Group Attribute	11	٢
	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	10

### Group Attribute and Access Control

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

7. Click VPN:

WatchGuard Firewa	ire XTM Web UI		Jser: admin   Help   Logout
DASHBOARD SYSTEM STATUS	Servers		
NETWORK FIREWALL	Authentication Servers		
SUBSCRIPTION SERVICES	Server	Status	
Hotspot	Firebox	0 Users	0 Groups
Servers Settings	RADIUS	Primary	10.0.10.130
Web Server Certificate		Secondary	Disabled
Terminal Services	SecurID	Primary	Disabled
SYSTEM		Secondary	Disabled
	LDAP	Primary	Disabled
		Secondary	Disabled
	Active Directory	0 domains	

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

WatchGuard Firewa	are XTM Web UI	Us	ser: admin   Help   Logout
DASHBOARD SYSTEM STATUS	Servers		
NETWORK FIREWALL	Authentication Servers		
SUBSCRIPTION SERVICES	Server	Status	
AUTHENTICATION VPN	Firebox	0 Users	2 Groups
Branch Office VPN BOVPN Virtual Interfaces	RADIUS	Primary	10.0.10.83
Phase2 Proposals Mobile VPN with IPSec		Secondary	Disabled
Mobile VPN With PPTP Mobile VPN with SSL Mobile VPN with L2TP Global Settings SYSTEM	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 Fire	ware XTM Web UI
DASHBOARD SYSTEM STATUS NETWORK FIREWALL SUBSCRIPTION SERVICES	Mobile VPN with IPSec  Groups  Name  Authentication Serv Allowed Access Virtual IP Pool IPSec Settings
AUTHENTICATION VPN Branch Office VPN BOVPN Virtual Interfaces Phase2 Proposals Mobile VPN with IPSec Mobile VPN with IPPTP Mobile VPN with SSL Mobile VPN with L2TP Global Settings SYSTEM	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

- 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.

User: admin   Help   Logout			
DASHBOARD SYSTEM STATUS NETWORK	Mobile VPN with IPSec / Add		
FIREWALL SUBSCRIPTION SERVICES AUTHENTICATION VPN	General IPSec Tunnel Resources Advanced		
Branch Office VPN BOVPN Virtual Interfaces Phase2 Proposals Mobile VPN with IPSec Mobile VPN with PPTP	General Settings Authentication Server RADIUS		
Mobile VPN with PPTP Mobile VPN with SSL Mobile VPN with L2TP Global Settings SYSTEM	Passphrase		
	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

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

Mobile VPN with IPSec group profile name

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

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

WatchGuard Firewa	re XTM Web UI User: admin   Help   Logout
DASHBOARD SYSTEM STATUS	Mobile VPN with IPSec / Add
	Name Office VPN
AUTHENTICATION	General IPSec Tunnel Resources Advanced
VPN Branch Office VPN BOVPN Virtual Interfaces Phase2 Proposals Mobile VPN with IPSec Mobile VPN with PPTP	General Settings Authentication Server RADIUS
Mobile VPN with SSL Mobile VPN with L2TP Global Settings SYSTEM	Passphrase Passphrase Confirm
	Firebox IP Addresses
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
	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**

12.

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. <u>Click here</u> 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

WatchGuard	Firewa	re XTM Web	UI			User: admir	n   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK		Front Panel					m <sup>e</sup>
FIREWALL		Top Clients				System	
SUBSCRIPTION SERVIC	CES	Name	Rate 🌲	Bytes	Hits	Name	XTM_2_Series-W
AUTHENTICATION	ŝ	10.0.88.100	531 Kbps	21 MB	21	Model	XTM26-W
VPN		10.0.88.104	211 Kbps 📒	9 MB	14	Version Serial Number	11.9.5.B470931 70A70CDC3D640
STSTEM		10.0.88.102	29 Kbps	9 MB	13	System Time	14:42 US/Eastern
		Top Destinatio	ns			System Date Uptime	2015-06-17 2 days 01:55

2. Click Servers

WatchGuard Firewa	re XTM Web L	Л			User: admir	n   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK	Front Panel					٢
FIREWALL	Top Clients				System	
SUBSCRIPTION SERVICES	Name	Rate 🜩	Bytes	Hits	Name	XTM 2 Series-W
AUTHENTICATION	10.0.88.100	151 Kbps	3 MB	22	Model	XTM26-W
Servers	10.0.88.104	105 Kbps	8 MB	118	Serial Number	11.9.5.B470931 70A70CDC3D640
Settings	10.0.88.102	28 Kbps	9 МВ	14	System Time	14:43 US/Eastern
Web Server Certificate Single Sign-On	Top Destination	S			System Date	2015-06-17 2 days 01:56
Terminal Services Authentication Portal	Name	Rate 🜩	Bytes	Hits	Log Server	Disabled
VPN	184.150.152.14	126 Kbps	2 MB	1	Reboot	
SYSTEM	74.125.29.101	20 Kbps	646 КВ	1		
	136.146.210.32	19 Kbps	177 КВ	2		
	184.150.152.18	18 Kbps	137 KB	2	Last 20 Mir	nutes 🛊

#### 3. Select RADIUS

WatchGuard Firew	are XTM Web UI	L	Jser: admin   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK FIREWALL	Servers Authentication Servers		
SUBSCRIPTION SERVICES	Server	Status	
AUTHENTICATION Hotspot Servers Settings Users and Groups Web Server Certificate Single Sign-On Terminal Services Authentication Portal VPN SYSTEM	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 Serv	ver Settings			
C Enable Seco	ndary RADIUS Se	erver		
	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 S	erver	
IP Address	10.0.10.131	
Port	1812	)
Passphrase		]
Confirm		]
Timeout	120	seconds
Retries	1	]
Group Attribute	11	]
Dead Time	10 Minutes \$	
Save		

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	1
Group Attribute	11
Dead Time	10 Minutes \$
Save	

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 etho
- 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 etho 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**:

ම Login <b>TC</b> 📭	inTC RADIUS Connector 2.1.0	🖹 Docs	📞 Support	💄 logintc-user 🗸
GENERAL	🔁 Status			
📥 Configurations				
🗐 Logs	All status checks have passed.			
APPLIANCE	t Ding cloud legists com			
🚯 Status				
Settings	✓ RADIUS Process			
Upgrade	✓ CPU Usage			
	✓ RAM Usage			
	✓ Disk Usage			
	✓ Version check			

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

FC RADIUS Connector 2.1.0	🔊 Docs 🌜 Support 🚨 logintc-user
🛢 Logs	
/var/log/logintc/authenticate.log /var/log/radius/radius.log	/var/log/logintc/tornado.log
2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.17, 2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.11, 2015-04-28 17:10:18,082 - INFO - 304 GET /configuratio 2015-04-28 17:10:18,082 - INFO - 304 GET /configuratio 2015-04-28 17:10:21,624 - INFO - 304 GET /configuratio 2015-04-28 17:10:22,004 - INFO - 304 GET /configuratio 2015-04-28 17:10:22,004 - INFO - 304 GET /configuratio 2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.11, 2015-04-28 17:10:22,39 - INFO - 304 GET /logs (10.0.11) 2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.11) 2015-04-28 17:10:20 - INFO - 304 GET /logs (10.0.11) 2015-04-28 17:10:20 - INFO - 304 GET /logs (10.0.11) 2015-04-28 - INFO - 304 GET /logs (10.0.11) 2015-04-28 - INFO - I	(%) 2.42ms .0.178) 2.59ms nns (10.0.10.178) 2.43ms (%) 2.43ms .10.178) 2.45ms nns (10.0.10.178) 2.40ms nns (10.0.10.178) 2.40ms .0.178) 2.22ms .0.178) 3.00ms 
	C RADIUS Connector 2.1.0

Unsuccessful authentication may be caused by premature timeouts

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

## **Email Support**

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

## **Incorrect Group Settings**

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

WatchGuard Firewa	re XTM Web	UI				User: admir	n   Help   Logout
DASHBOARD Englishing SYSTEM STATUS	Front Panel						S
FIREWALL	Top Clients					System	
SUBSCRIPTION SERVICES	Name	Rate 🜩	By	tes	Hits	Name	XTM_2_Series-W
AUTHENTICATION	10.0.88.104	166 Kbps 🔜	11 MB		64	Model	XTM26-W
VPN	10.0.88.100	107 Kbps 📒	720 KB		37	Version Serial Number	11.9.5.B470931 70A70CDC3D640
STOLEM	10.0.88.102	73 Kbps 📕	9 MB		17	System Time	14:52 US/Eastern
	Top Destinatio	ns				System Date Uptime	2015-06-17 2 days 02:05

Log Server

Disabled

#### Click on Traffic Monitor:

WatchGuard Firewa	are XTM Web L	וו			User: admir	n   Help   Logout
DASHBOARD Front Panel Subscription Services FireWatch Interfaces	Front Panel				System	۵
Traffic Monitor Gatew Wireless Controller SYSTEM STATUS NETWORK FIREWALL	Name 10.0.88.104 10.0.88.100 10.0.88.102	Rate 🜩 138 Kbps 🗾 61 Kbps 📕 35 Kbps 📕	Bytes 11 MB 873 KB 10 MB	Hits 57 36 14	Name Model Version Serial Number System Time	XTM_2_Series-W XTM26-W 11.9.5.B470931 70A70CDC3D640 14:53 US/Eastern
SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM	Top Destination Name 184.150.152.15 74.125.22.139	Rate 🜩	Bytes	Hits 3	System Date Uptime Log Server Reboot	2015-06-17 2 days 02:06 Disabled
	10.0.10.164	14 Kbps	11 MB	2		

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

WatchGuard Firew	are XTM Web UI	User: admin   Help   Logout
DASHBOARD Front Panel Subscription Services FireWatch Interfaces Traffic Monitor Gateway Wireless Controller SYSTEM STATUS NETWORK FIREWALL SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM	Traffic Monitor 2015-06-17 15:03:23 sessiond sessiond: sessiond WGAPI call 2015-06-17 15:03:23 sessiond sessiond: wgapi: rcved cmd=1 //toS 2015-06-17 15:03:23 sessiond sessiond: get into sess_prcs_status 2015-06-17 15:03:23 sessiond oKI sess update oK, sessId=28 2015-06-17 15:03:26 Deny 10.0.10.176 10.0.10.255 netbios-ns/ud 2015-06-17 15:03:26 Deny 10.0.10.176 10.0.10.255 netbios-ns/ud 2015-06-17 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff.62 IEEE 80 2015-06-17 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff.62 IEEE 80 2015-06-17 15:03:32 hostapd ath1: STA 7c:d1:c3:7b:ff.62 IEEE 80 2015-06-17 15:03:37 Deny 10.0.88.100 255.255.255 17:500/u 2015-06-17 15:03:39 Deny 10.0.20.30 10.0.10.1 dns/udp 58082 5 2015-06-17 15:03:43 iked ******* RECV message on fd_server(7) 2015-06-17 15:03:43 sessiond sessiond: sessiond WGAPI call 2015-06-17 15:03:43 sessiond sessiond: sessiond WGAPI call 2015-06-17 15:03:43 sessiond sessiond: wgapi: rcved cmd=7 //pin2 2015-06-17 15:03:43 sessiond	Sessiond/updateActivity' fromIPC=-61236 s(): xpath=/toSessiond/updateActivity p 137 137 0-External Firebox Denied 78 02.11: authenticated 02.11: associated (aid 3) vairwise key handshake completed (RSN) dp 17500 17500 1-WG-Wireless-Access- 3 0-External Firebox Denied 51 63 (Unha 3 0-External Firebox Denied 55 63 (Unha ) ******* iss it

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

settings:

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

Search for the following error message:

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

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

ි Login <b>TC</b>	LoginTC RADIUS Connector 2.1.1	🗐 Docs 🕓 Support 🖀 logintc-user 🕶
GENERAL	🚓 Configurations	Restart RADIUS Server + Create
🖧 Configurations		
🗐 Logs	test-radius-1 (TestDomain)	✓ Test Configuration
APPLIANCE	()) m RADIUS	
🚯 Status		
🗱 Settings		
🗐 Upgrade		

Click the Edit Button in the First Factor section:

ම Login <b>TC</b> යැ	ginTC RADIUS Connector 2.1.1	🖻 Docs 🕓 Support 🔒 logintc-user 🗸
GENERAL	A Configurations / to	est-radius-1 Test Configuration Back Delete
Logs		The 40-character domain ID is found on the LoginTC Admin Panel domain settings page.
APPLIANCE		LØ Edit
<ul><li>ℬ Status</li><li>✿ Settings</li></ul>	First Factor Select the first way users will	○ LDAP <ul> <li>○ Active Directory</li> <li>○ RADIUS</li> <li>○ None</li> </ul> Connect to an existing Active Directory server for username / password verification.
🕑 Upgrade	authenticate prior to LoginTC.	Car Edit 👆
	Passthrough	No Passthrough Static List LDAP Group Active Directory Group
	Configure list of users which will not be challenged by	All authentications will be challenged with LoginTC. This can be configured at anytime.

Scroll down to the to the Group Attribute section:

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



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

ခာ Login <b>TC</b> မ	ginTC RADIUS Connector 2.1.1	🗟 Docs 🕓 Support 🚢 logintc-user 🗸					
GENERAL	🛔 Edit Configuration	A / First Factor Cancel					
Configurations		The attribute containing the user's email address. Examples: mail or email.					
APPLIANCE	Group Attribute (Advanced)	လက္ဆ None 💿 Specify a Group Attribute RADIUS Group Attribute					
Status	Specify an additional user group attribute to be returned	filter-id					
<ul> <li>Settings</li> <li>Upgrade</li> </ul>	the authenticating server.	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-ld.					
		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** :

WatchGuard Firew	vare XTM Web UI User: admin   Help	o   Logout
DASHBOARD SYSTEM STATUS	Traffic Monitor	П
NETWORK		٩
SUBSCRIPTION SERVICES	2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)******** RECV an IKE packet at 10.0.10 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)ike_match_if_name: Match pcy [Rando 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)ike_match_if_name: Match pcy [L2TP-I	).8:500(socket mR_mu] dev= IPSec_l2] dev=
VPN Branch Office VPN BOVPN Virtual Interfaces Phase2 Proposals	2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)Found IKE Policy [KandomK_mu, dev= 2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)IkeNotess Notify Payload NtoH : SPI Size 16 firs 2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)Process Notify Payload : NOTIFY-TYPi 2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)Process ISAKMP Notify : from peer 0x0 2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)Process ISAKMP Notify : from peer 0x0	tanyEj for peer st4(0x95b5255 E : 36136 0a000a8c proto
Mobile VPN with IPSec Mobile VPN with PPTP Mobile VPN with SSL	2015-06-17 15:04:23 iked (10.0.10.8<>>10.0.10.140)Received DPD R_U_THERE message 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)IkeInNotifyProcess: gateway is UP (pee 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)ike_p1_status_chg: ikePcyName=Rand 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)ikeMultiWanVpnFailBack: ->	rrom 10.0.10.1 erip=10.0.10.1 iomR_mu, stat
Mobile VPN With L2TP Global Settings SYSTEM	2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)MWAN-Failback muvpn case, do nothin 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)IkeNotifyPayloadHtoN : net order spi(0x 2015-06-17 15:04:23 iked (10.0.10.8<->10.0.10.140)Sending DPD R_U_THERE_ACK mess 2015-06-17 15:04:43 iked ******** RECV message on fd_server(7) *******	ng - name=Rar k95 0xb5 0x25 sage to 10.0.10
	2015-06-17 15:04:43 iked recv CMD XPATH(/ping), need to process it	

#### Click on the Authentication tab:

WatchGuard Firewa	are 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 SLL Mobile VPN with L2TP Global Settings SYSTEM	Mobile VPN with SSL When you activate Mobile VPN with SSL, the " policy are created to allow Mobile VPN with SS Activate Mobile VPN with SSL General Authentication Advanced Firebox IP Addresses or Domain Names Type a firebox IP or domain name for SSL VPN Primary 10.0.10.83 Secondary	SSLVPN-Users" group and the "WatchGuard SSLVPN" L connections from the Internet to the external interface.
	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	Туре	Authentication Server			
	SSLVPN-Users Group Any					
Add	Remove					
Sav	a .					

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

Mobile VPN with Global Settings	L2TP RADIUS (De	fault)	Automation berrer		
SYSTEM	Add User or Grou	ıp		×	
	Туре	• Group User			
	Name	GroupName			s you define are
	Authentication Server	RADIUS	¢		
			ОК	Cancel	

# 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** 

WatchGuard	Firewa	re XTM Web	UI			User: admir	n   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK FIREWALL		Front Panel				System	n.
SUBSCRIPTION SERVI AUTHENTICATION VPN SYSTEM	ices	Name 10.0.88.100 10.0.88.104 10.0.88.102	Rate 🖨	Bytes 21 MB 9 MB 9 MB	Hits 21 14 13	Name Model Version Serial Number System Time	XTM_2_Series-W XTM26-W 11.9.5.B470931 70A70CDC3D640 14:42 US/Eastern
		Top Destinatio	ns			System Date Uptime	2015-06-17 2 days 01:55

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

WatchGuard Firewa	re XTM Web L	II			User: admir	n   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK	Front Panel					٢
FIREWALL	Top Clients				System	
SUBSCRIPTION SERVICES	Name	Rate 🔶	Bytes	Hits	Name	XTM 2 Series-W
AUTHENTICATION Hotspot	10.0.88.100	151 Kbps	3 MB	22	Model Version	XTM26-W 11.9.5.B470931
Setfuls Setfuls Users and Groups	<u>10.0.88.104</u> <u>10.0.88.102</u>	28 Kbps	9 MB	14	Serial Number System Time	70A70CDC3D640 14:43 US/Eastern
Web Server Certificate Single Sign-On	Top Destination	S			System Date Uptime	2015-06-17 2 days 01:56
Terminal Services	Name	Rate 🜩	Bytes	Hits	Log Server	Disabled
VPN	184.150.152.14	126 Kbps 🔜	2 MB	1	Reboot	
SYSTEM	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	Last 20 Mir	nutes 🛊

#### 2. Click **RADIUS**

WatchGuard Firew	are XTM Web UI		User: admin   Help   Logout
DASHBOARD SYSTEM STATUS NETWORK FIREWALL SUBSCRIPTION SERVICES	Servers Authentication Servers	Status	
AUTHENTICATION	Server	Ollsers	2 Groups
Hotspot Servers Settings	RADIUS	Primary	10.0.10.83
Users and Groups Web Server Certificate	<	Secondary	Disabled
Single Sign-On Terminal Services Authentication Portal VPN	SecurID	Primary	Disabled
		Secondary	Disabled
SYSTEM	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 Firev	are XTM Web UI	Logout
DASHBOARD SYSTEM STATUS	Servers / RADIUS	
NETWORK FIREWALL SUBSCRIPTION SERVICES	Before you configure your XTM device to use a RADIUS authentication server, make sure the successfully accept and process RADIUS authentication requests.	server can
AUTHENTICATION	Primary Server Settings Primary Enable RADIUS Server	
Servers Settings	IP Address 10.0.10.83	
Users and Groups Web Server Certificate Single Sign-On	Port 1812	
Terminal Services Authentication Portal	Passphrase	
VPN SYSTEM	Confirm	
	Timeout 120 Seconds	

See the <u>Knowledge Base</u> 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?