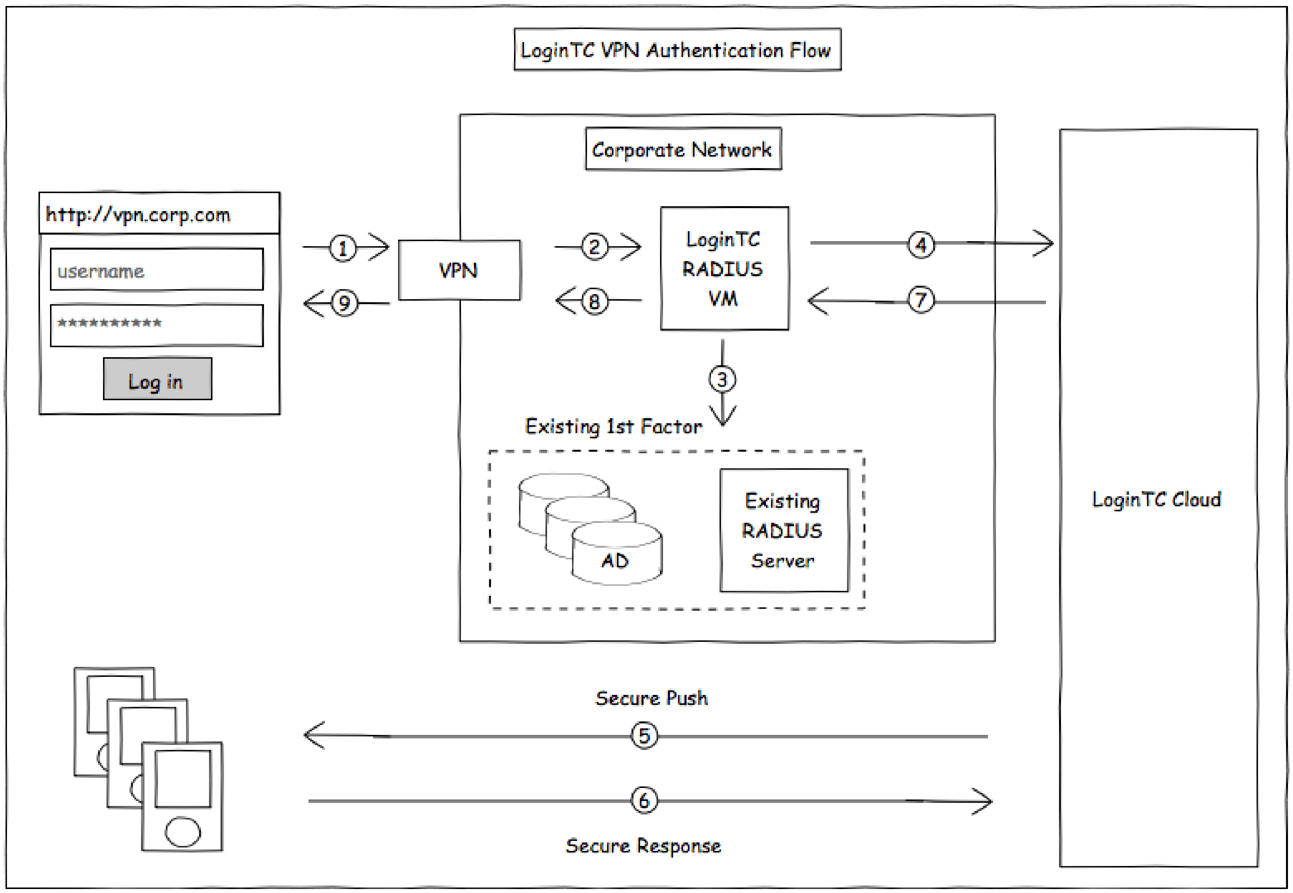
Two factor authentication for Fortinet SSL VPN

logintc.com/docs/connectors/fortinet.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 Fortinet SSL VPN to use LoginTC for the most secure two-factor authentication.



Compatibility

Fortinet appliance compatibility:

- FortiGate/FortiWifi 30-90 Entry-Level series
- FortiGate 100-900 Mid-Range series
- FortiGate 1000-5000 High-End series
- Fortinet/FortiGate appliance supporting RADIUS authentication

Appliance not listed?

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

Compatibility Guide

Fortinet appliances which have configurable RADIUS authentication are supported.

Prerequisites

Before proceeding, please ensure you have the following:

RADIUS Domain Creation

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

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

   Create Domain

4. Enter domain information:

   Create Domain Form

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

   Connector
   RADIUS

Installation

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

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

Note: Username and Password

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

The `logintc-user` has `sudo` privileges.

Configuration

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

1. LoginTC

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

2. First Factor

This section describes how the appliance will conduct an optional first factor. Either against an existing LDAP, Active Directory or RADIUS server. If no first factor is selected, then only LoginTC will be used for authentication (since there are 4-digit PIN and Passcode options that unlock the tokens to access your domains, LoginTC-only authentication this still provides two-factor authentication).

3. Passthrough

This section describes whether the appliance will perform a LoginTC challenge for an authenticating user. The default is to challenge all users. However with either a static list or Active Directory / LDAP Group you can control whom gets challenged to facilitate seamless testing and rollout.

4. Client and Encryption

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

Data Encryption

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

The **web interface** makes setting up a configuration simple and straightforward. Each section has a **Test** feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

First Configuration

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

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

Web Server

LoginTC Settings

Configure which LoginTC organization and domain to use:

Web Server

Configuration values:

Property	Explanation
`api_key`	The 64-character organization API key
`domain_id`	The 40-character domain ID

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

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

Web Server

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.

Web Server

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**:

Web Server

Configuration values:

Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`

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

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**:

Web Server

Configuration values:

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

RADIUS Vendor-Specific Attributes

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

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

Passthrough

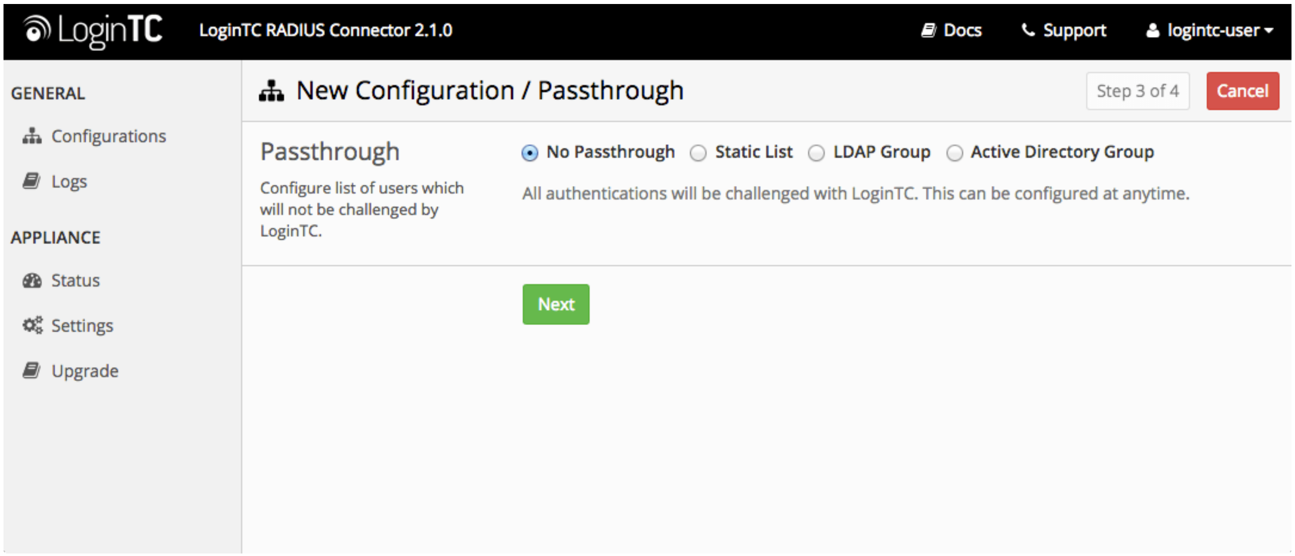
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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

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

No Passthrough (default)

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



Passthrough

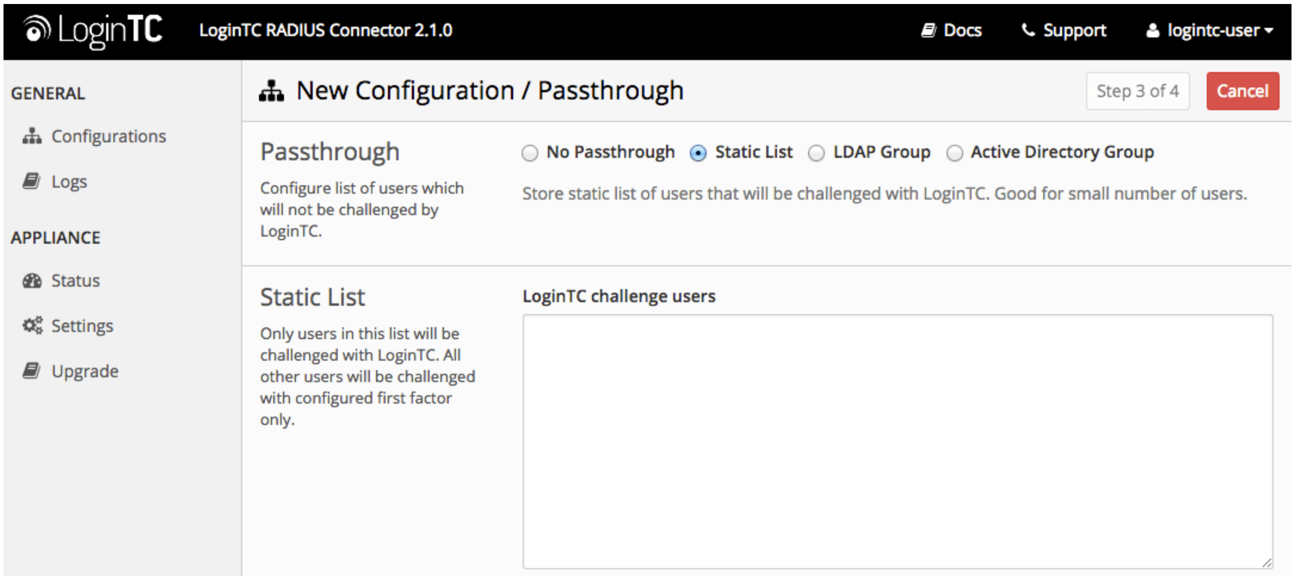
Configure list of users which will not be challenged by LoginTC.

● No Passthrough ○ Static List ○ LDAP Group ○ Active Directory Group

All authentications will be challenged with LoginTC. This can be configured at anytime.

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.



New Configuration / Passthrough

Passthrough

Configure list of users which will not be challenged by LoginTC.

○ No Passthrough ● Static List ○ LDAP Group ○ Active Directory Group

Store static list of users that will be challenged with LoginTC. Good for small number of users.

Static List

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

LoginTC challenge users

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

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

Active Directory / LDAP Group

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

Web Server

Configuration values:

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

Property	Explanation	Examples
`attr_email`	The attribute containing the user’s email address	`mail` or `email`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

Configuration Simplified

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

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

Client and Encryption

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

Web Server

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`

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**.

Web Server

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:

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

Web Server

Click **Test Configuration**:

Web Server

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:

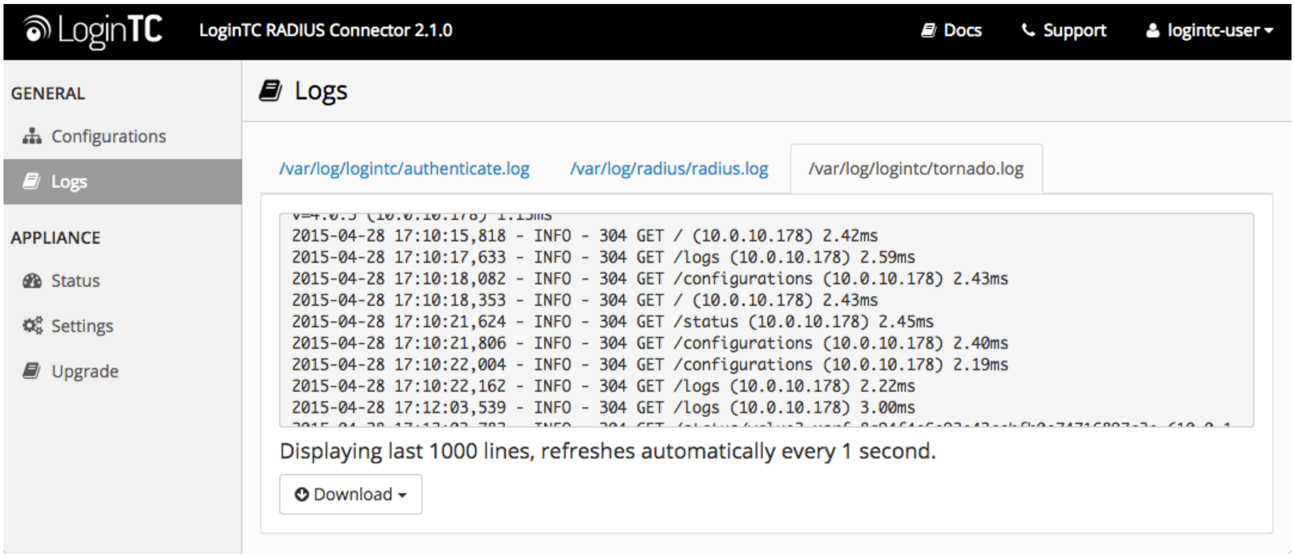
Web Server

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:

Web Server

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


LoginTC
LoginTC RADIUS Connector 2.1.0
Docs
Support
logintc-user
GENERAL
Configurations
Logs
APPLIANCE
Status
Settings
Upgrade
Logs
/var/log/logintc/authenticate.log
/var/log/radius/radius.log
/var/log/logintc/tornado.log

```
v=4.0.5 (10.0.10.178) 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 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms
2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms
2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms
2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms
2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms
```

Displaying last 1000 lines, refreshes automatically every 1 second.

Fortinet Configuration - Quick Guide

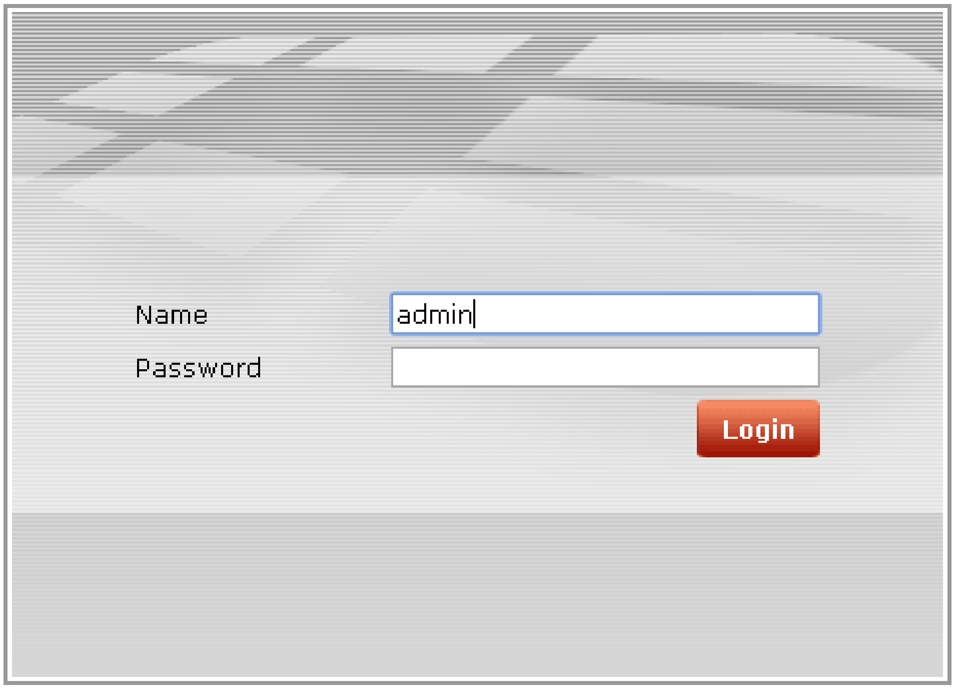
Once you are satisfied with your setup, configure your Fortinet to use the LoginTC RADIUS Connector.

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

Web Server

The following are quick steps to get VPN access protected with LoginTC. The instructions can be used for existing setups as well.

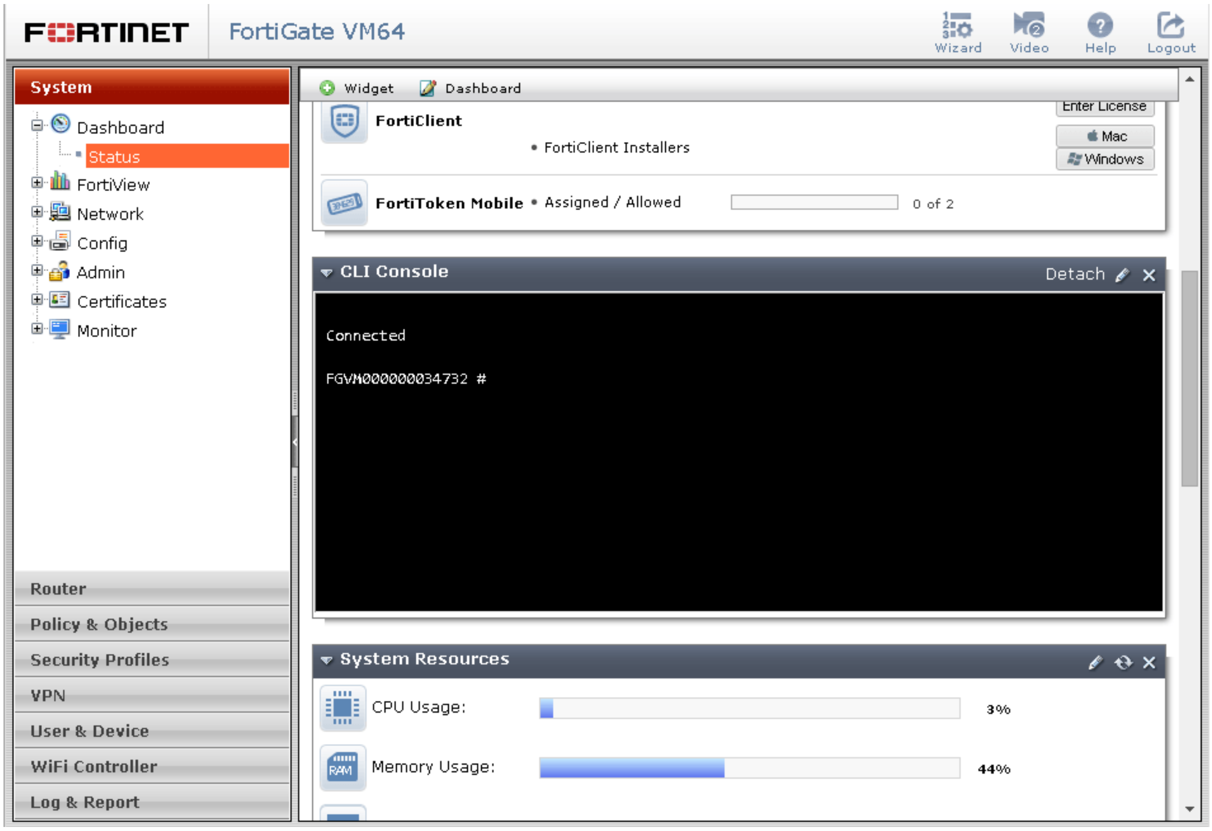
1. Sign In to your Fortinet web manager (https://<IP address for the Fortinet web manager>)



Name: admin

Password:

2. Navigate to **System** > **Dashboard** > **Status** and scroll down to **CLI Console**:



FortiClient
- FortiClient Installers

FortiToken Mobile
- Assigned / Allowed 0 of 2

CLI Console

```
Connected

FGVM000000034732 #
```

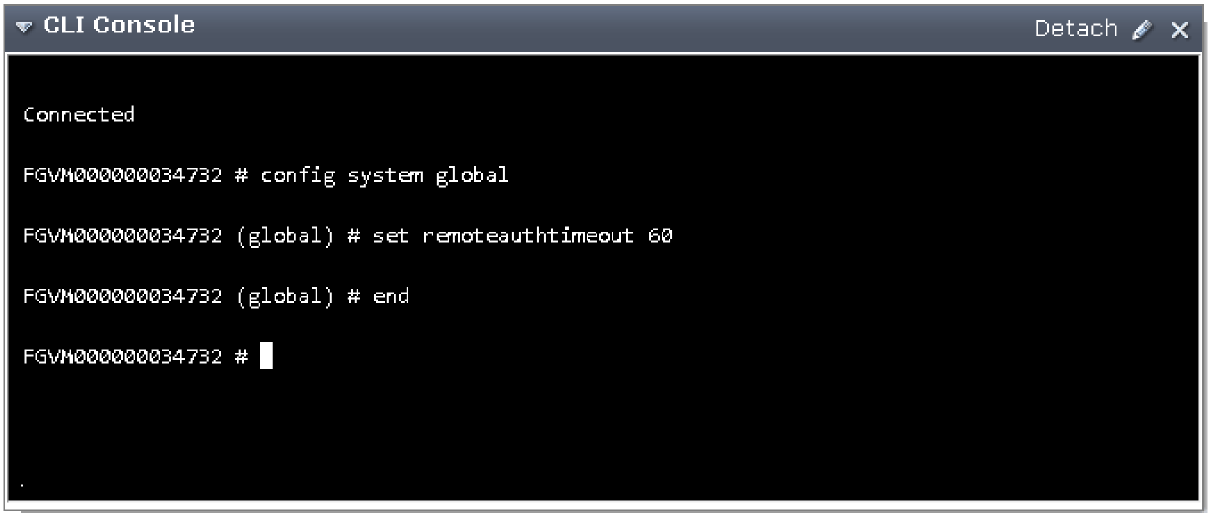
System Resources

CPU Usage: 3%

Memory Usage: 44%

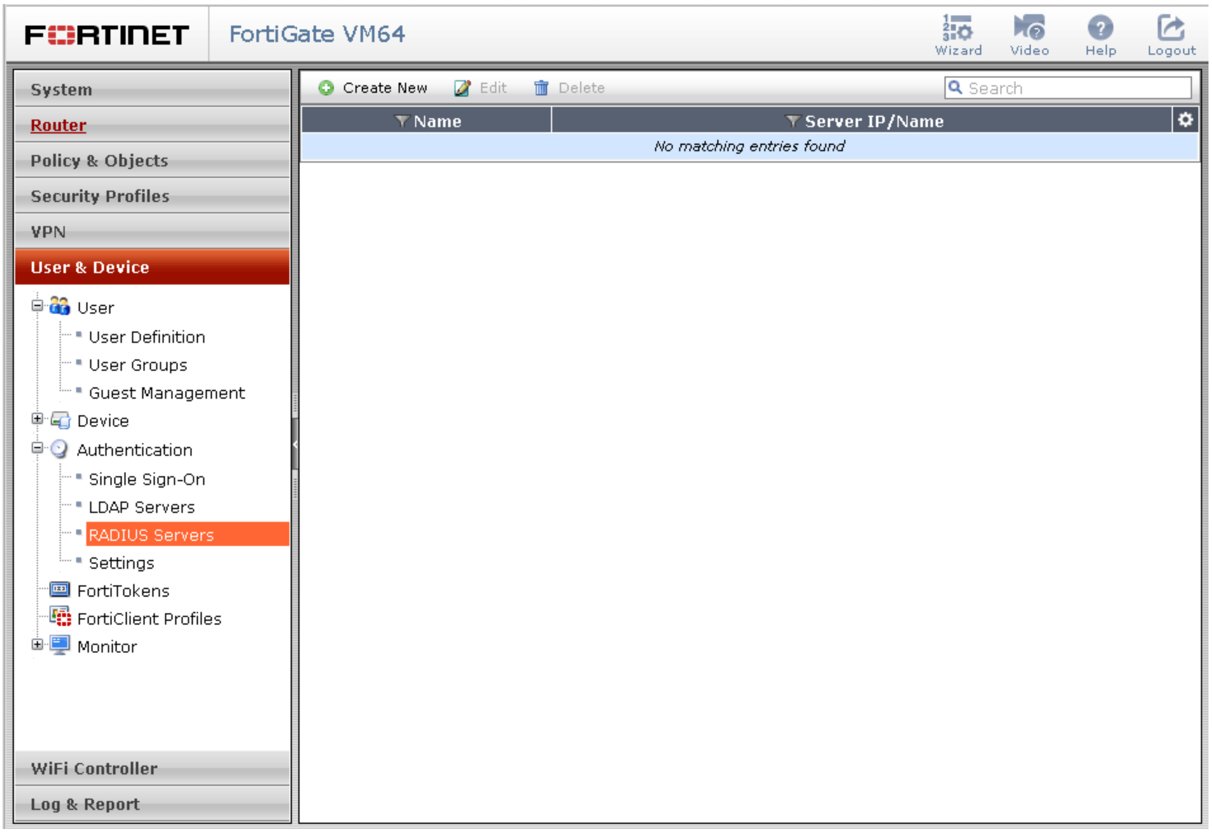
3. Run the following commands in the console:

```
# config system global
# set remoteauthtimeout 90
# end
```



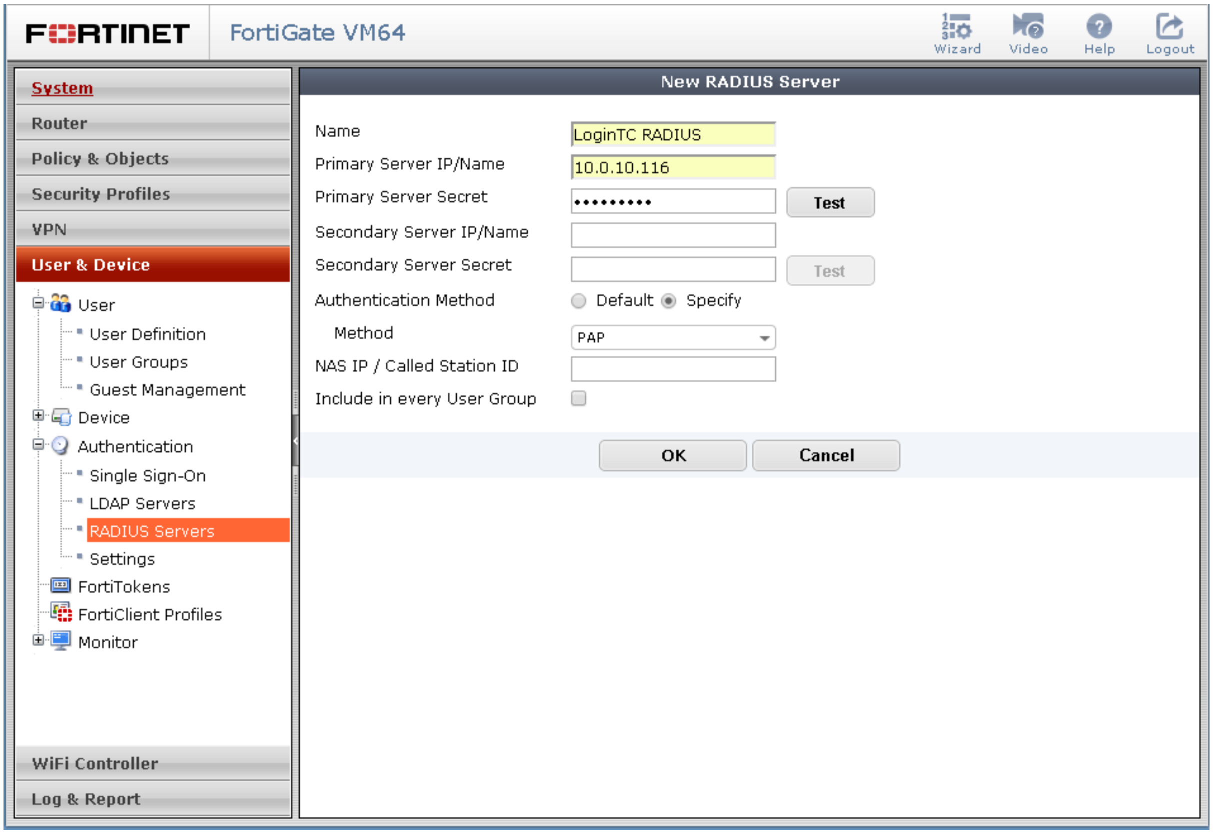
```
Connected

FGVM000000034732 # config system global

FGVM000000034732 (global) # set remoteauthtimeout 60

FGVM000000034732 (global) # end

FGVM000000034732 #
```

4. Navigate to **User & Device** > **Authentication** > **RADIUS Servers** and click on **Create New** button:



No matching entries found

5. Complete the form and click **OK** (click the **Test** button beside **Primary Server Secret** to test the setup):



New RADIUS Server

Name	LoginTC RADIUS
Primary Server IP/Name	10.0.10.116
Primary Server Secret	•••••••••
Secondary Server IP/Name	
Secondary Server Secret	
Authentication Method	○ Default ● Specify
Method	PAP
NAS IP / Called Station ID	
Include in every User Group	☐

Property	Explanation	Example
`Primary Server IP/Name`	Address of LoginTC RADIUS Connector	`10.0.10.116`
`Primary Server Secret`	The secret shared between the LoginTC RADIUS Connector and its client.	`bigsecret`
`Secondary Server IP/Name`	Secondary RADIUS Server IP. Optional.	
`Secondary Server Secret`	The secondary server secret. Optional.	
`Authentication Method`	RADUIS authentication method. Must be PAP.	`PAP`
`NAS IP / Called Station ID`	Network Access Server IP. Optional.	
`Include in every User Group`	Automatically included in all user groups. Optional.	

To test, navigate to your Fortinet VPN portal and attempt access.

Troubleshooting

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
   ```

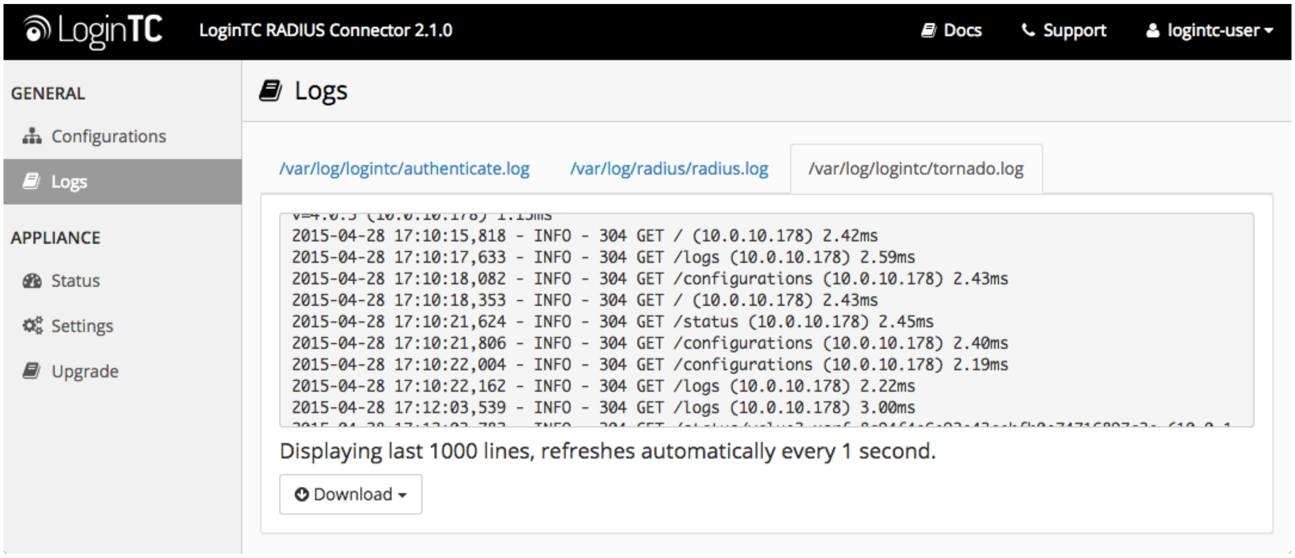
   Open the file and update the `DEVICE="eth0"` line to `DEVICE="eth1"`

Not Authenticating

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

Web Server

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


LoginTC
LoginTC RADIUS Connector 2.1.0
Docs
Support
logintc-user
GENERAL
Configurations
Logs
APPLIANCE
Status
Settings
Upgrade
Logs
/var/log/logintc/authenticate.log
/var/log/radius/radius.log
/var/log/logintc/tornado.log

```
v=4.0.3 (10.0.10.178) 1.13ms
2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms
2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms
2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms
2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms
2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms
2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms
2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms
2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms
2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms
```

Displaying last 1000 lines, refreshes automatically every 1 second.

Email Support

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