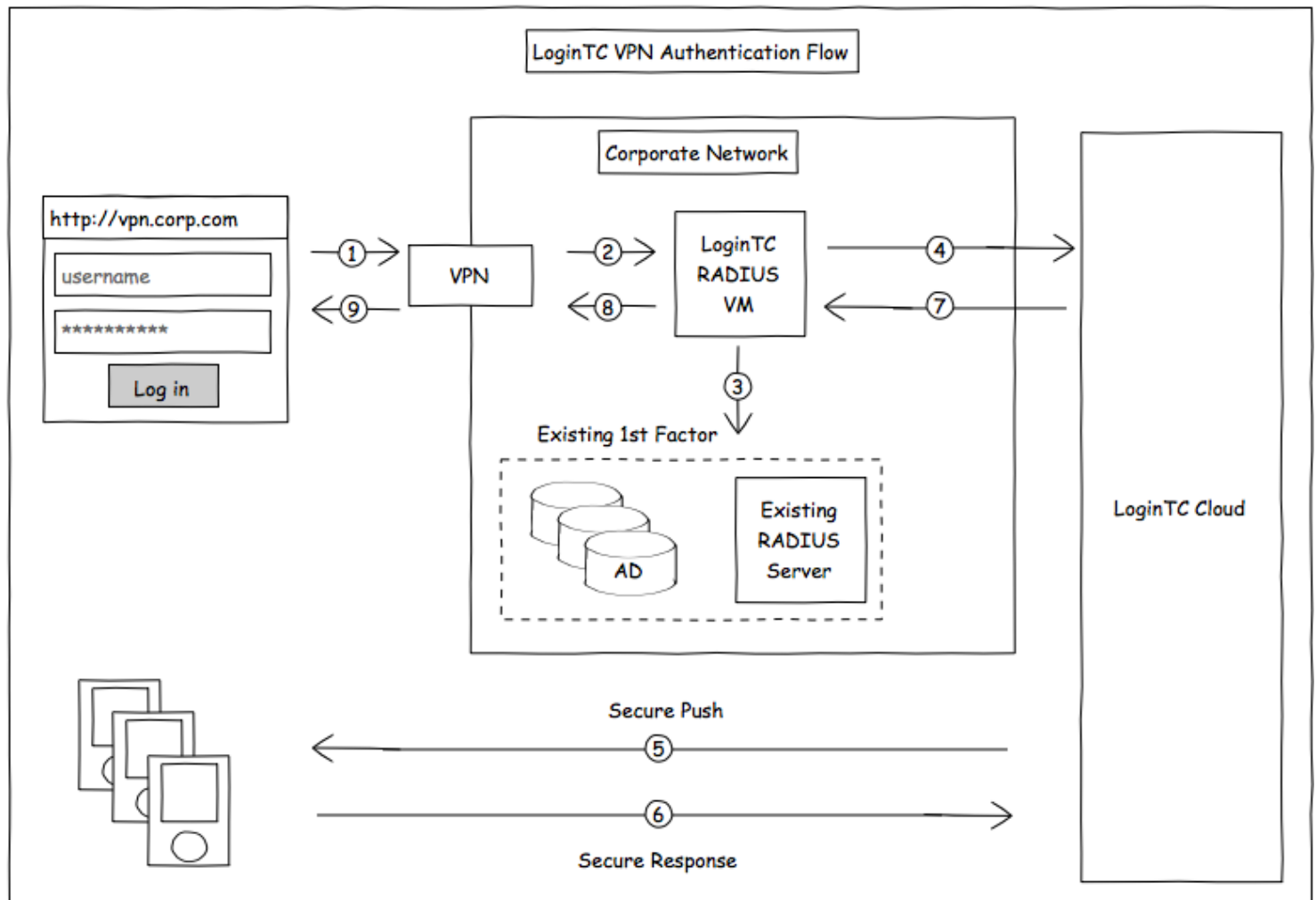


# Two factor authentication for Cisco ASA SSL VPN

[www.logintc.com/docs/connectors/cisco-asa.html](http://www.logintc.com/docs/connectors/cisco-asa.html)

## Introduction

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables Cisco ASA to use LoginTC for the most secure two-factor authentication.



## Compatibility

Cisco ASA appliance compatibility:

- Cisco ASA 5505
- Cisco ASA 5506 Series
- Cisco ASA 5508-X
- Cisco ASA 5512-X
- Cisco ASA 5515-X
- Cisco ASA 5516-X

- Cisco ASA 5525-X
- Cisco ASA 5545-X
- Cisco ASA 5555-X
- Cisco ASA 5585-X Series
- Cisco appliance supporting RADIUS authentication

## Compatibility Guide

Any other Cisco appliance which have configurable RADIUS authentication are supported.

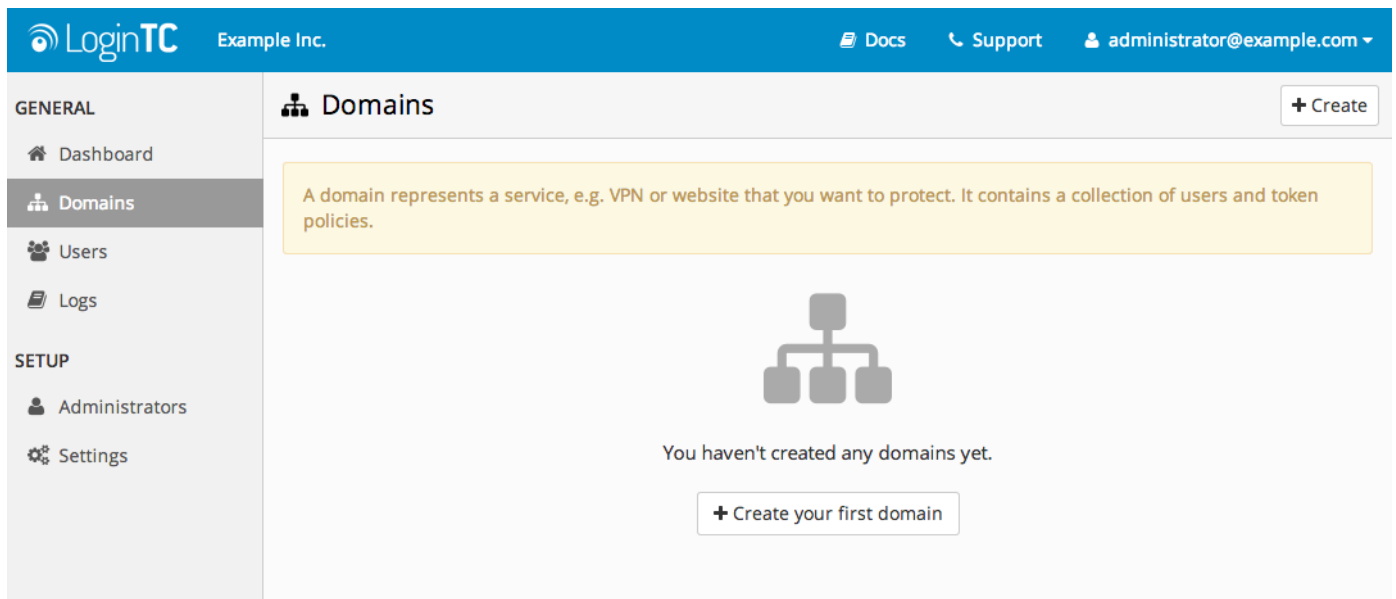
## Prerequisites

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**:



4. Enter domain information:

Example Inc.

Docs
Support
administrator@example.com

GENERAL

Dashboard

**Domains**
Users
Logs

SETUP

Administrators
Settings

Domains / Create Domain
Cancel

Name

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

Icon

Default
Custom

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

Connector

RADIUS
API
OpenAM
SiteMinder
Drupal
WordPress
Joomla

How you will connect your infrastructure to this domain

RADIUS

Use the [RADIUS Connector](#) for your RADIUS appliance

Key Policy

PIN
Passcode

Specify how your users will unlock their token to authenticate

Note: if you are already using passwords for the first factor, we recommend PIN

Create

Name

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

Connector

RADIUS

## Installation

The LoginTC RADIUS Connector runs [CentOS 6.5](#) with [SELinux](#). A firewall runs with the following open ports:

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

3/21

## 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 changed.

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

## Configuration

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

### 1. LoginTC

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

### 2. First Factor

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

### 3. Passthrough

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

### 4. Client and Encryption

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

## Data Encryption

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

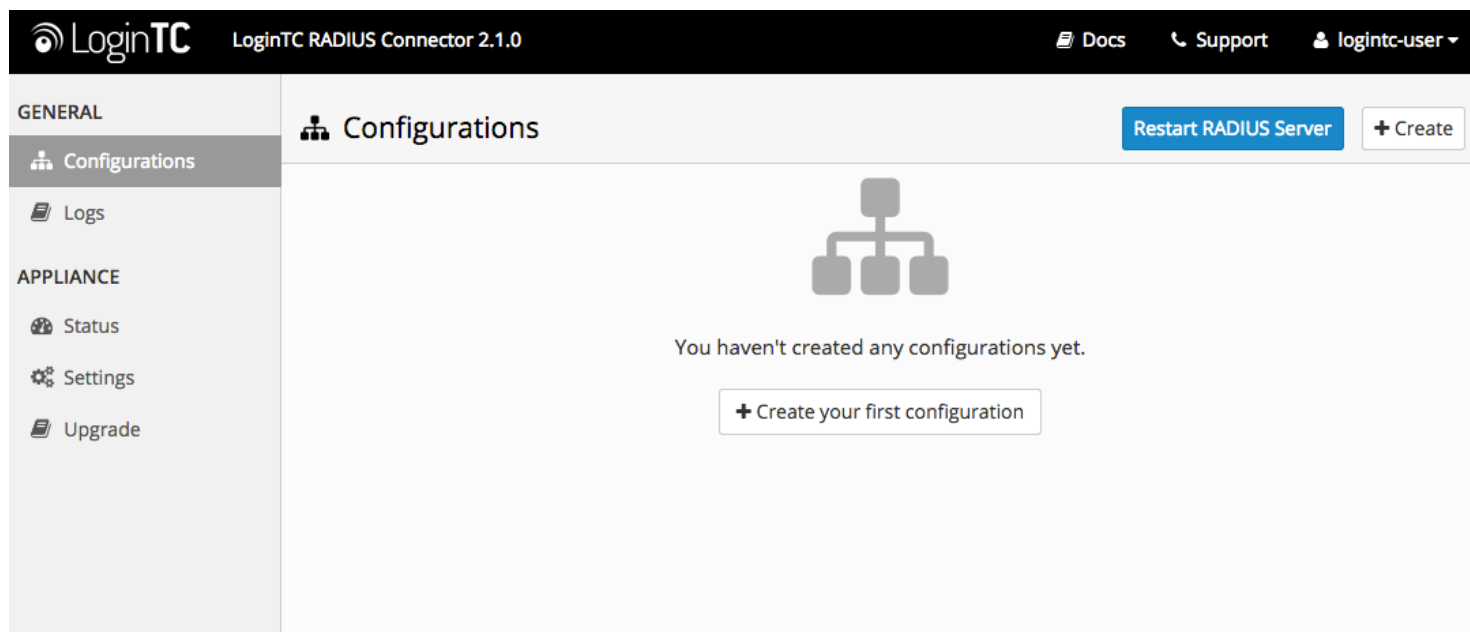
The **web interface** makes setting up a configuration simple and straightforward. Each section has a **Test** feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

## First Configuration

Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the

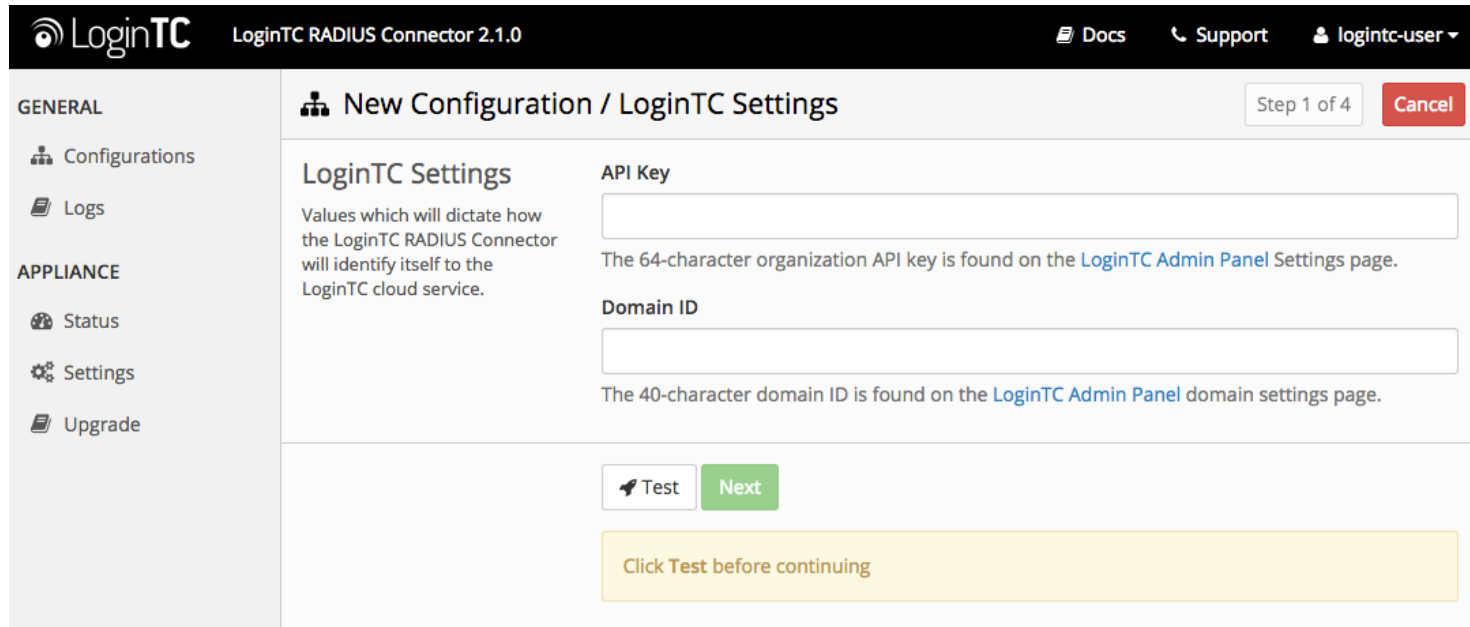
password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



## LoginTC Settings

Configure which LoginTC organization and domain to use:



Configuration values:

`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**:

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**New Configuration / LoginTC Settings** Step 1 of 4 **Cancel**

**LoginTC Settings**

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

**API Key**

vZkDw7l6Z3tApwZjXERseKdR0s5RNNqjMxXlwvxpWwJOa9oJXi9b5tdvPyFsQzWj

The 64-character organization API key is found on the [LoginTC Admin Panel](#) Settings page.

**Domain ID**

9120580e94f134cb7c9f27cd1e43dbc82980e152

The 40-character domain ID is found on the [LoginTC Admin Panel](#) domain settings page.

**Test** **Next**

Test successful, click **Next** to continue

## First Authentication Factor

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

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

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

**First Factor**

☒ LDAP ☐ Active Directory ☐ RADIUS ☐ None

Select the first way users will authenticate prior to LoginTC. Connect to an existing LDAP server for username / password verification.

**LDAP Server Details**

The LDAP host and port information.

**Host**

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

**Port (optional)**

389

Port if LDAP server uses non-standard port.

**Bind Details**

☒ Bind with credentials ☐ Anonymous

## Active Directory / LDAP Option

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

LoginTC RADIUS Connector 2.1.0
 

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

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

New Configuration / First Factor

Step 2 of 4

Cancel

First Factor

LDAP

Active Directory

RADIUS

None

Select the first way users will authenticate prior to LoginTC.
 Connect to an existing Active Directory server for username / password verification.

AD Server Details

Host

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

Port (optional)

Port if Active Directory server uses non-standard port.

Bind Details

Bind with credentials

Anonymous

Configuration values:

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
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**.

7/21

## Existing RADIUS Server Option

If you want to use your existing RADIUS server, select **RADIUS**:

LoginTC

LoginTC RADIUS Connector 2.1.0

Docs

Support

logintc-user

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

New Configuration / First Factor

Step 2 of 4

Cancel

First Factor

LDAP

Active Directory

☒ RADIUS

None

Select the first way users will authenticate prior to LoginTC.

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

RADIUS Server Details

The RADIUS host and secret.

Host

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

Port (optional)

1812

Port if the RADIUS server uses non-standard port.

Secret

Configuration values:

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)	6812
secret	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	testing123

## RADIUS Vendor-Specific Attributes

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

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

## Passthrough

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

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

For larger deployments you can elect to use the [Active Directory or LDAP Group](#) option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC

your LDAP and Active Directory group policy will ensure that they will be challenged with LoginTC. Users not part of the group will only be challenged with the configured [First Authentication Factor](#).

## No Passthrough (default)

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

The screenshot shows the 'New Configuration / Passthrough' screen in the LoginTC RADIUS Connector 2.1.0. The left sidebar has 'GENERAL' selected, with sub-items 'Configurations' and 'Logs'. Under 'APPLIANCE', there are 'Status', 'Settings', and 'Upgrade'. The main content area is titled 'New Configuration / Passthrough' and shows 'Step 3 of 4'. The 'Passthrough' section has four radio buttons: 'No Passthrough' (selected), 'Static List', 'LDAP Group', and 'Active Directory Group'. Below the radio buttons, it says 'Configure list of users which will not be challenged by LoginTC.' and 'All authentications will be challenged with LoginTC. This can be configured at anytime.' A green 'Next' button is visible.

## Static List

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


The screenshot shows the 'New Configuration / Passthrough' screen in the LoginTC RADIUS Connector 2.1.0. The left sidebar is the same as the previous screenshot. The main content area shows 'Step 3 of 4'. The 'Passthrough' section has four radio buttons: 'No Passthrough', 'Static List' (selected), 'LDAP Group', and 'Active Directory Group'. Below the radio buttons, it says 'Configure list of users which will not be challenged by LoginTC.' and 'Store static list of users that will be challenged with LoginTC. Good for small number of users.' The 'Static List' section is expanded, showing a description: 'Only users in this list will be challenged with LoginTC. All other users will be challenged with configured first factor only.' Below this is a text area labeled 'LoginTC challenge users' for entering a list of usernames.

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

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

## Active Directory / LDAP Group

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

 LoginTC RADIUS Connector 2.1.0

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

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

New Configuration / Passthrough

Step 3 of 4 Cancel

Passthrough

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

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

Connect to an existing Active Directory server for group membership verification. Good for large number of users.

Auth Groups

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

LoginTC challenge Auth Groups

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

AD Server Details

The Active Directory host and port information.

Host

Configuration values:

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
attr_email	The attribute containing the user's email address	mail or email

<code>encryption</code> (optional)	Encryption mechanism	<code>ssl</code> or <code>startTLS</code>
<code>cacert</code> (optional)	CA certificate file (PEM format)	<code>/opt/logintc/cacert.pem</code>

## Configuration Simplified

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

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

## Client and Encryption

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

**GENERAL**

- Configurations
- Logs

**APPLIANCE**

- Status
- Settings
- Upgrade

**New Configuration / Client and Encryption** Step 4 of 4 **Cancel**

**Client Settings**

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

**Name**

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

**IP Address**

The IP address of your RADIUS client.

**Secret**

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

**Encryption**

☒ **Encrypt all passwords and API keys**

Determine whether to store passwords and API keys encrypted or in the clear. It is strongly recommended to encrypt all sensitive fields.


Client configuration values:

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


## 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**.

 LoginTC

LoginTC RADIUS Connector 2.1.0

 Docs

 Support

 logintc-user ▾

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings


Upgrade

Configurations

Restart RADIUS Server

+ Create

Configuration office-vpn-1 created

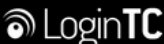
 office-vpn-1 (Office VPN)  
RADIUS

Test Configuration


## 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:

 LoginTC

LoginTC RADIUS Connector 2.1.0

 Docs

 Support

 logintc-user ▾

GENERAL

Configurations

Logs

APPLIANCE

Status


Settings

Upgrade

Configurations

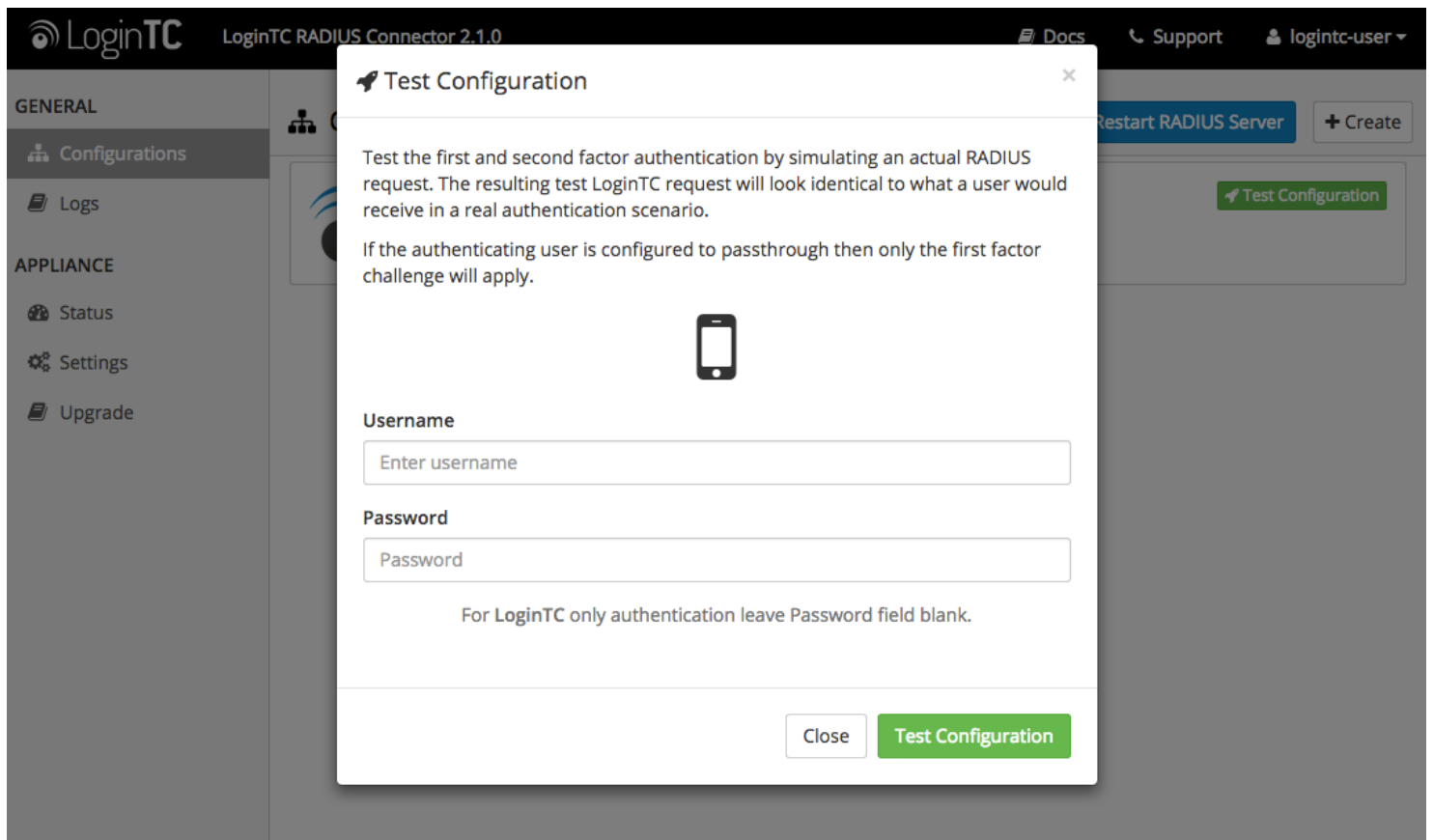
Restart RADIUS Server

+ Create

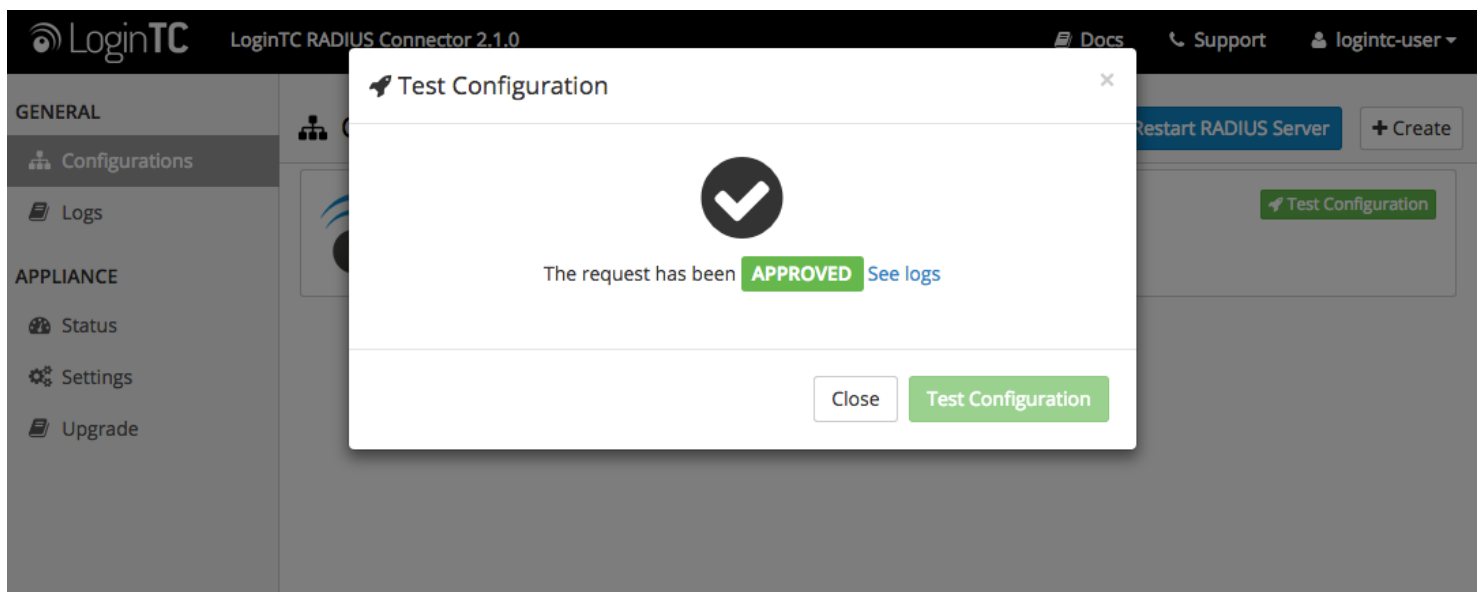
 office-vpn-1 (Office VPN)  
RADIUS

Test Configuration

Click **Test Configuration**:

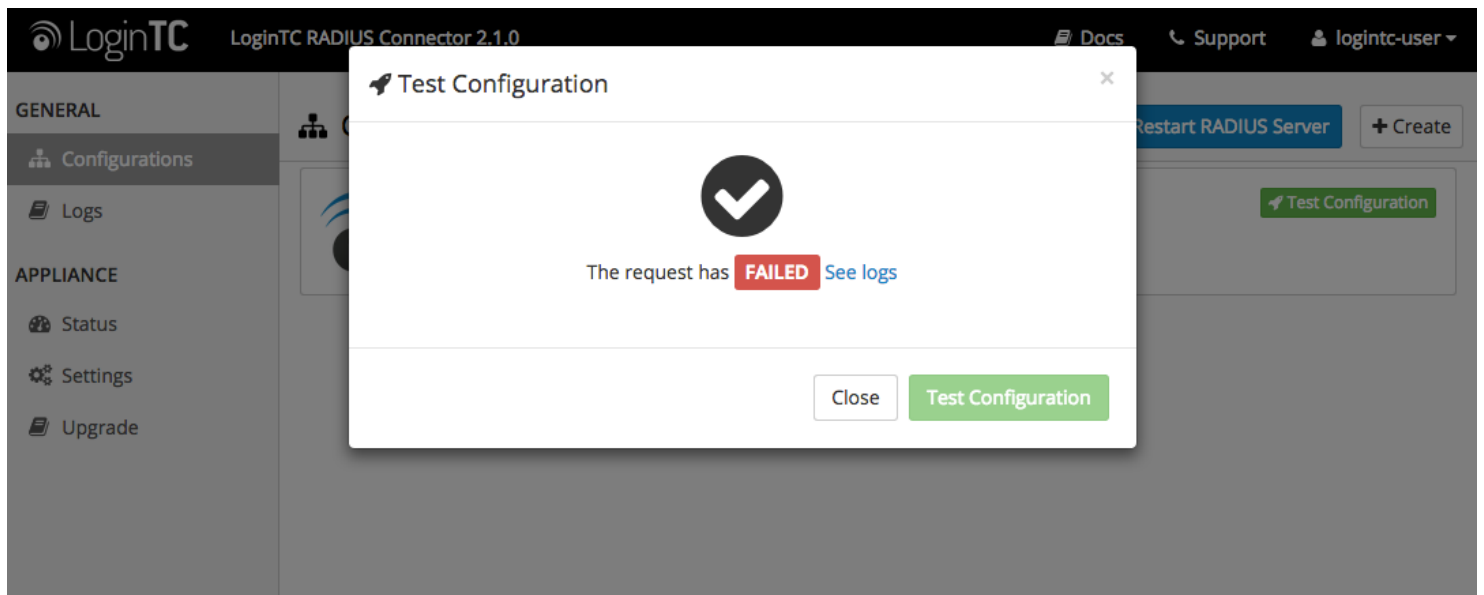


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

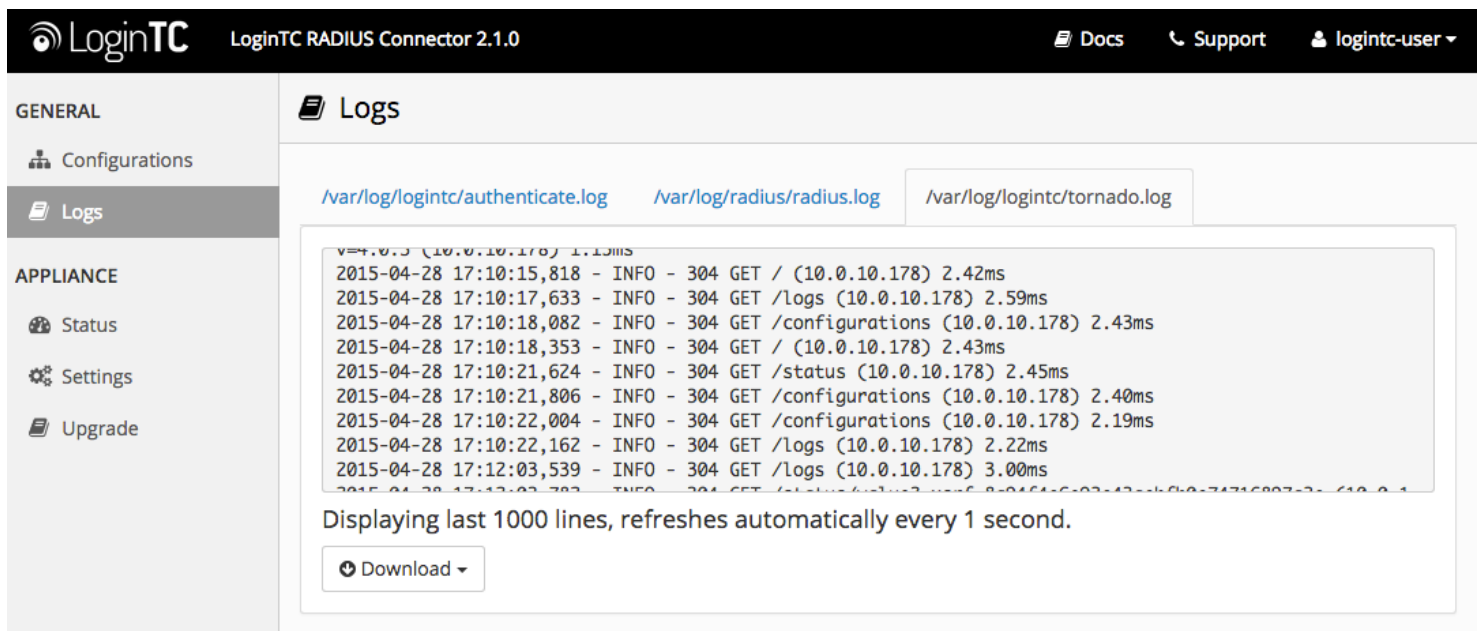


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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




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



## Cisco ASA Configuration - Quick Guide

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

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

 LoginTC

LoginTC RADIUS Connector 2.1.0

Docs

Support

logintc-user

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

Settings

Appliance

IP Address	10.0.10.116
RADIUS Authentication Port	1812
RADIUS Accounting Port	1813

The following are quick steps to protect your clientless and AnyConnect VPN setups with LoginTC. The instructions (tailored for Cisco ASA AnyConnect 2.5) can be used for existing setups as well.

1. Launch your Cisco ASA ASDM
2. Click **AAA Local Users** :

Cisco ASDM 6.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Look For:  Go

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration -> Remote Access VPN -> AAA Local Users -> AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
LoginTC	RADIUS	Single	Depletion	10	1

Find:

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.1.7	inside	60

Find:

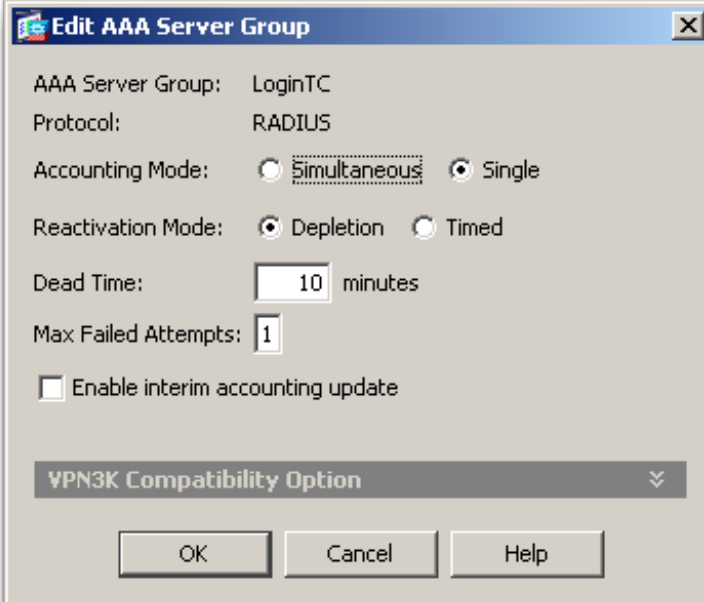
LDAP Attribute Map

Apply Reset

Configuration changes saved successfully.

<admin> 15 5/5/14 6:26:42 AM UTC

3. Under **AAA Server Groups** click **Add**:



**Edit AAA Server Group**

AAA Server Group: LoginTC

Protocol: RADIUS

Accounting Mode: ☐ Simultaneous ☒ Single

Reactivation Mode: ☒ Depletion ☐ Timed

Dead Time: 10 minutes

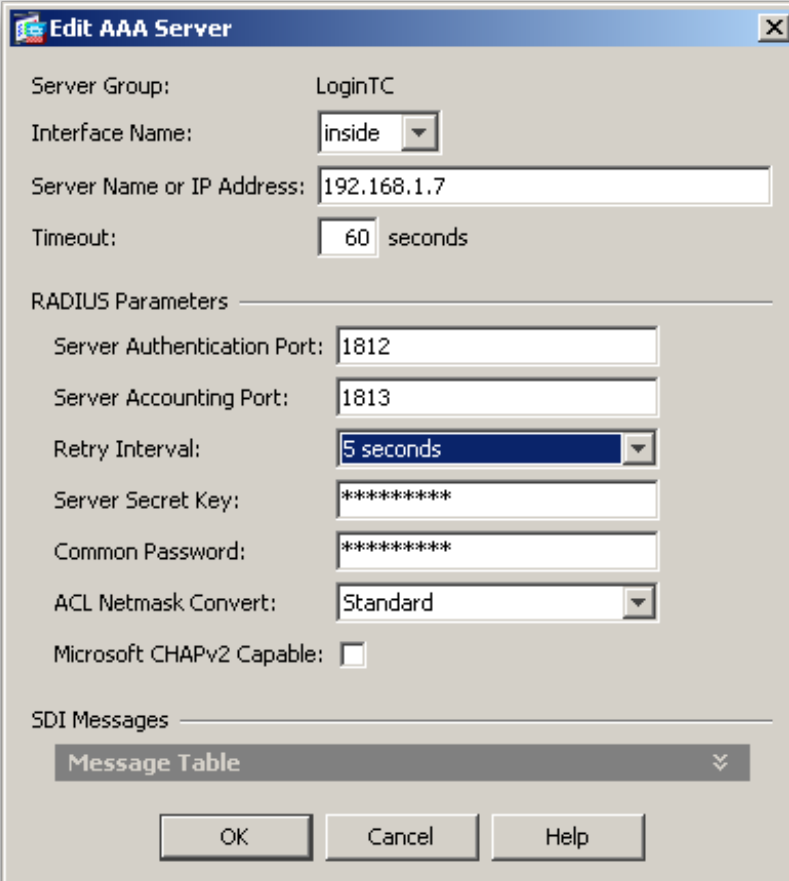
Max Failed Attempts: 1

☐ Enable interim accounting update

VPN3K Compatibility Option

OK Cancel Help

4. Select **Protocol**: RADIUS
5. Click **Add**
6. Select the newly created group
7. Under **Servers in the Selected Group** click **Add**:



**Edit AAA Server**

Server Group: LoginTC

Interface Name: inside

Server Name or IP Address: 192.168.1.7

Timeout: 60 seconds

**RADIUS Parameters**

Server Authentication Port: 1812

Server Accounting Port: 1813

Retry Interval: 5 seconds

Server Secret Key: \*\*\*\*\*

Common Password: \*\*\*\*\*

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☐

**SDI Messages**

Message Table

OK Cancel Help

Interface Name	Name of protected Cisco interface	inside
Server name or IP Address	Address of your LoginTC RADIUS Connector	192.168.1.7
Timeout	Authentication timeout period. Recommend 60s.	60
Server Authentication Port	RADIUS authentication port. Must be 1812.	1812
Server Accounting Port	RADIUS accounting port. Must be 1813	1813
Retry Interval	Length of time between retries	5
Server Secret Key	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret

8. Click **Clientless SSL VPN Access**:
9. Click **Connection Profiles**:
10. Select **DefaultWEBVPNGroup**, click **Edit**:

**Edit Clientless SSL VPN Connection Profile: anyconnect**

**Basic**  
 + Advanced

Name: anyconnect  
 Aliases: AnyConnect

**Authentication**  
 Method: ☒ AAA ☐ Certificate ☐ Both  
 AAA Server Group: LoginTC Manage...  
☐ Use LOCAL if Server Group fails

**DNS**  
 Server Group: DefaultDNS Manage...  
 (Following fields are attributes of the DNS server group selected above.)  
 Servers:   
 Domain Name: cisco

**Default Group Policy**  
 Group Policy: DfltGrpPolicy Manage...  
 (Following field is an attribute of the group policy selected above.)  
☒ Enable clientless SSL VPN protocol

Find:   
 Next Previous  
 OK Cancel Help

11. For the **AAA Server Group** select group made in steps 3-5

12. Click **OK**

## Configure Timeout

By default, the Cisco AnyConnect client will timeout after 12 seconds on Windows and after 30 seconds on Mac OS X. Your users may require more time to authenticate, so the following steps will guide you in creating a profile to override the default timeout.

To test, navigate to your Cisco ASA clientless VPN portal and attempt access.

## Warning: Connection Timeouts

The new profile will be downloaded and applied only after you have successfully connected the first time. If you are

having trouble with timeouts, we recommend that you connect using the clientless interface and clicking on the **Start AnyConnect** link to redownload the client. Also ensure that the FQDN and IP Address is correct in the **Server List**.

## User Management

There are several options for managing your users within LoginTC:

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

## Troubleshooting

### Connection Times Out After 12 Seconds

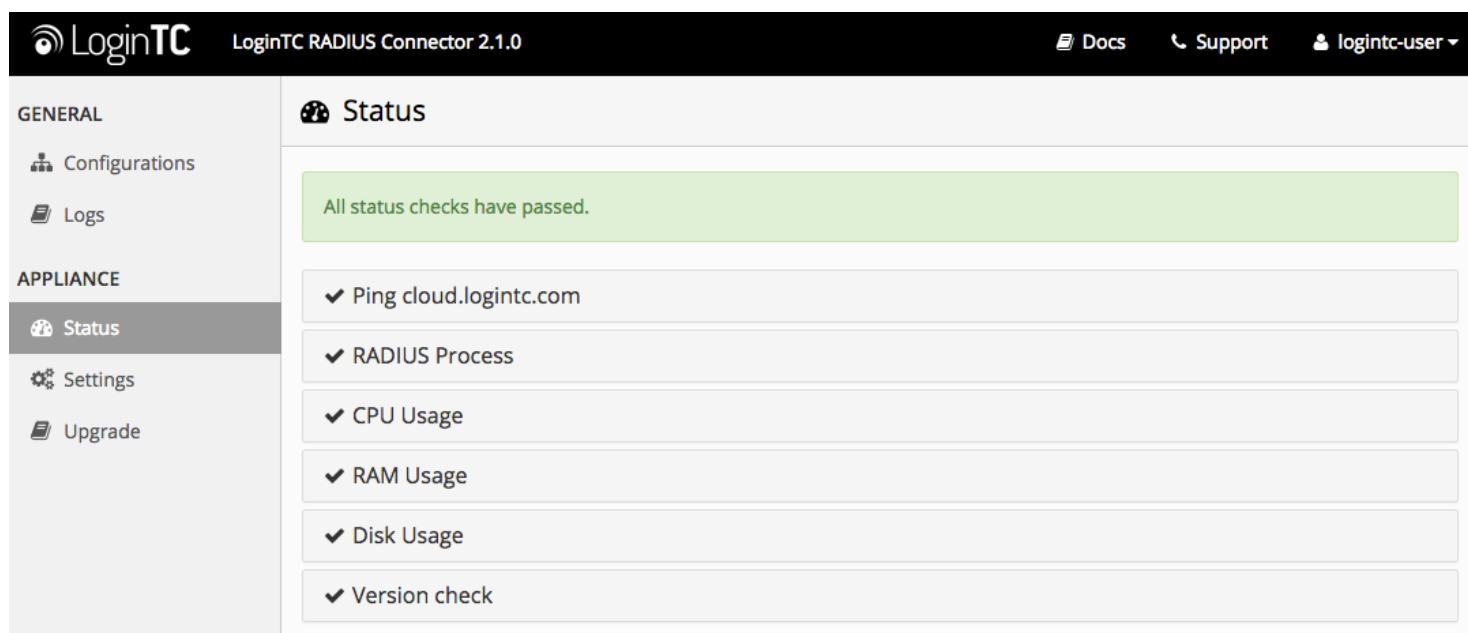
Ensure that you have configured the [AnyConnect Client Profile](#). Also ensure that the profile Hostname is the same hostname that your end-users use to connect to the VPN.

### Receiving Multiple Requests

Ensure that you have configured the [AnyConnect Client Profile](#). Also ensure that the profile Hostname is the same hostname that your end-users use to connect to the VPN.

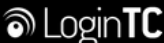
### Not Authenticating

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



The screenshot shows the LoginTC web interface. The top navigation bar includes the LoginTC logo, the version 'LoginTC RADIUS Connector 2.1.0', and links for 'Docs', 'Support', and a user profile 'logintc-user'. The left sidebar has two main sections: 'GENERAL' with links for 'Configurations' and 'Logs', and 'APPLIANCE' with links for 'Status', 'Settings', and 'Upgrade'. The 'Status' page is active, displaying a green message box that says 'All status checks have passed.' Below this, there is a list of status checks, each with a green checkmark icon and a text label: 'Ping cloud.logintc.com', 'RADIUS Process', 'CPU Usage', 'RAM Usage', 'Disk Usage', and 'Version check'.

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

 LoginTC

LoginTC RADIUS Connector 2.1.0

Docs

Support

logintc-user

GENERAL

Configurations

Logs

APPLIANCE

Status

Settings

Upgrade

Logs

/var/log/logintc/authenticate.log

/var/log/radius/radius.log

/var/log/logintc/tornado.log

2015-04-28 17:10:15,818 - INFO - 304 GET / (10.0.10.178) 2.42ms

2015-04-28 17:10:17,633 - INFO - 304 GET /logs (10.0.10.178) 2.59ms

2015-04-28 17:10:18,082 - INFO - 304 GET /configurations (10.0.10.178) 2.43ms

2015-04-28 17:10:18,353 - INFO - 304 GET / (10.0.10.178) 2.43ms

2015-04-28 17:10:21,624 - INFO - 304 GET /status (10.0.10.178) 2.45ms

2015-04-28 17:10:21,806 - INFO - 304 GET /configurations (10.0.10.178) 2.40ms

2015-04-28 17:10:22,004 - INFO - 304 GET /configurations (10.0.10.178) 2.19ms

2015-04-28 17:10:22,162 - INFO - 304 GET /logs (10.0.10.178) 2.22ms

2015-04-28 17:12:03,539 - INFO - 304 GET /logs (10.0.10.178) 3.00ms

Displaying last 1000 lines, refreshes automatically every 1 second.

Download

## Email Support

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