Two factor authentication for Cisco ASA SSL VPN Alternative

🔘 **logintc.com**/docs/connectors/cisco-asa-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 Cisco ASA to use LoginTC for the most secure two-factor authentication. For an alternate method using Challenge Response then you may be interested in: Two factor authentication for Cisco ASA SSL VPN Alternative.

User Experience

After entering the username and password into the AnyConnect 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. This flow works the same for clientless access.

Architecture
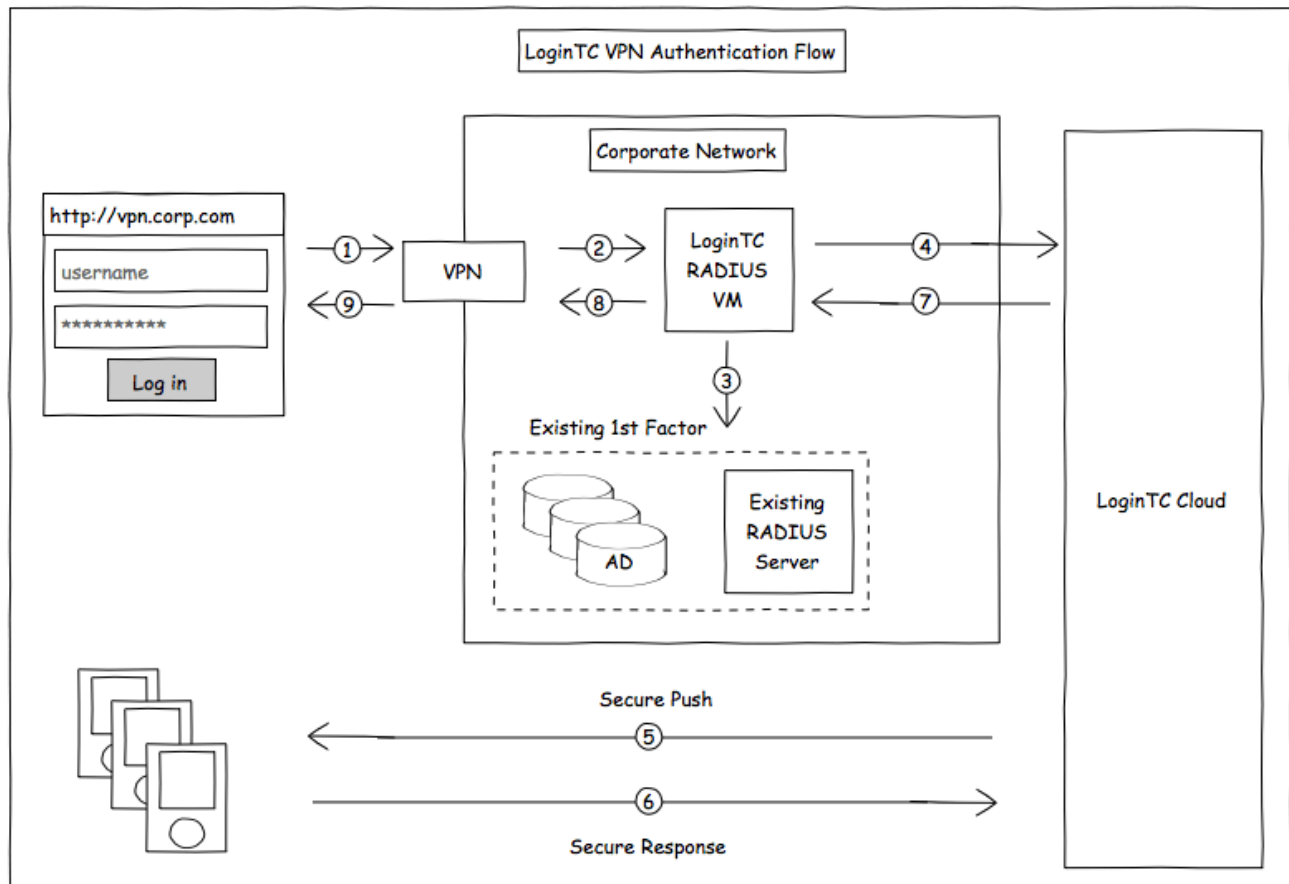
Compatibility

Cisco ASA appliance compatibility:

- Cisco ASA 5505
- Cisco ASA 5506-X Series
- Cisco ASA 5508-X
- Cisco ASA 5510-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

Appliance not listed?

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

Compatibility Guide

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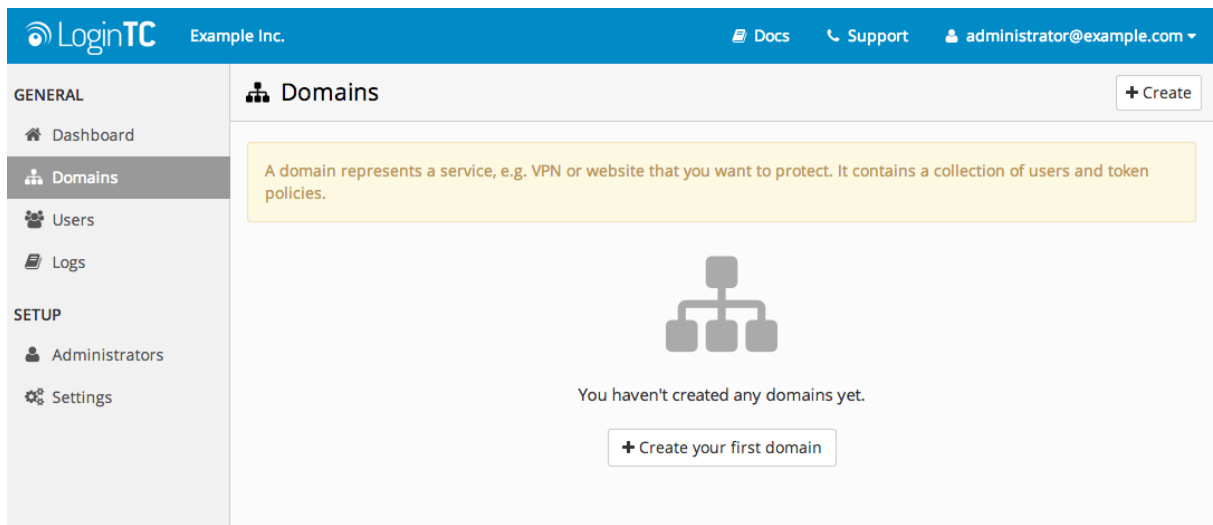
Prerequisites

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:

Name

Choose a name to identify your LoginTC Admin 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)
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 changed.

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

Data Encryption

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

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

First Configuration

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

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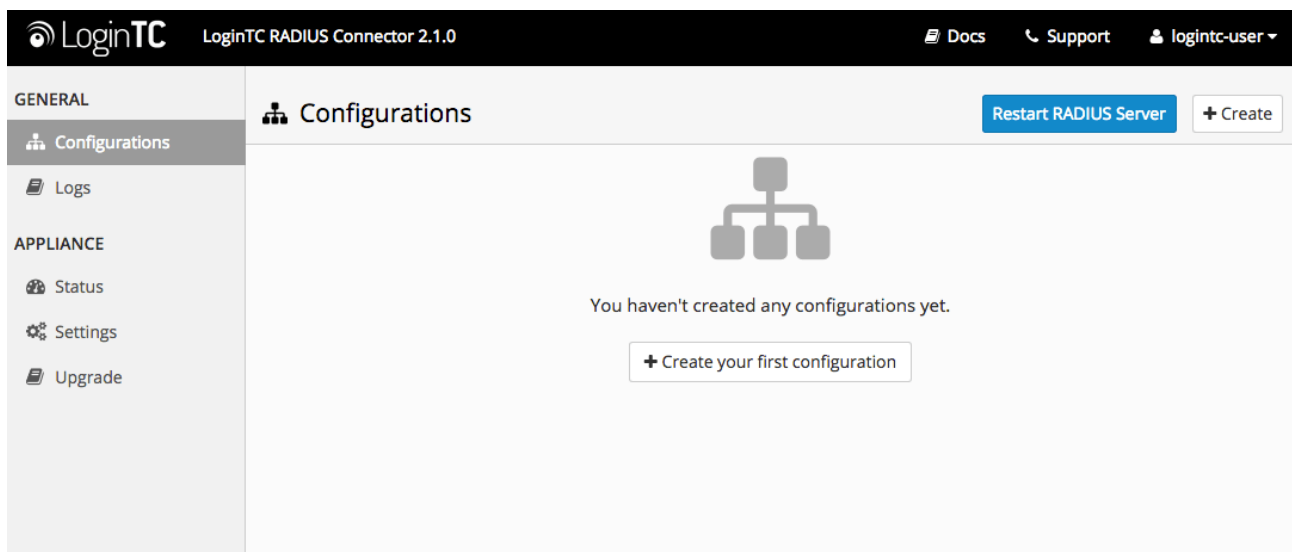
LoginTC Settings

Configure which LoginTC organization and domain to use:

Configuration values:

Property	Explanation
API Key	The 64-character organization API key
Domain ID	The 40-character domain ID
`Request Timeout `	Number of seconds that the RADIUS connector will wait for

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

Request Timeout

Make a note of what you set the Request Timeout to as you will need to use a larger timeout value in your Cisco ASA. 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 Cisco ASA.

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

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.

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**:

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`

Property	Explanation	Examples
`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**:

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.

Static List

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

LoginTC 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.

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`
`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):

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**

The LoginTC RADIUS Connector will directly and automatically perform the LoginTC second factor. See User Experience 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**.
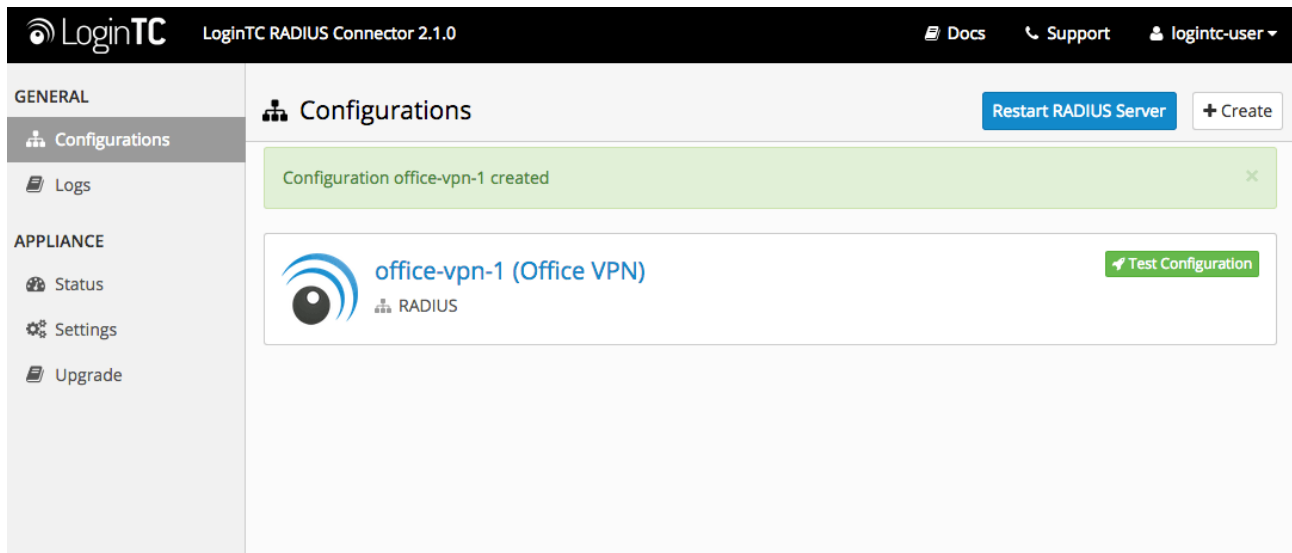
Testing

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

When you have loaded a token for your new user and domain, navigate to your appliance**web interface** URL:
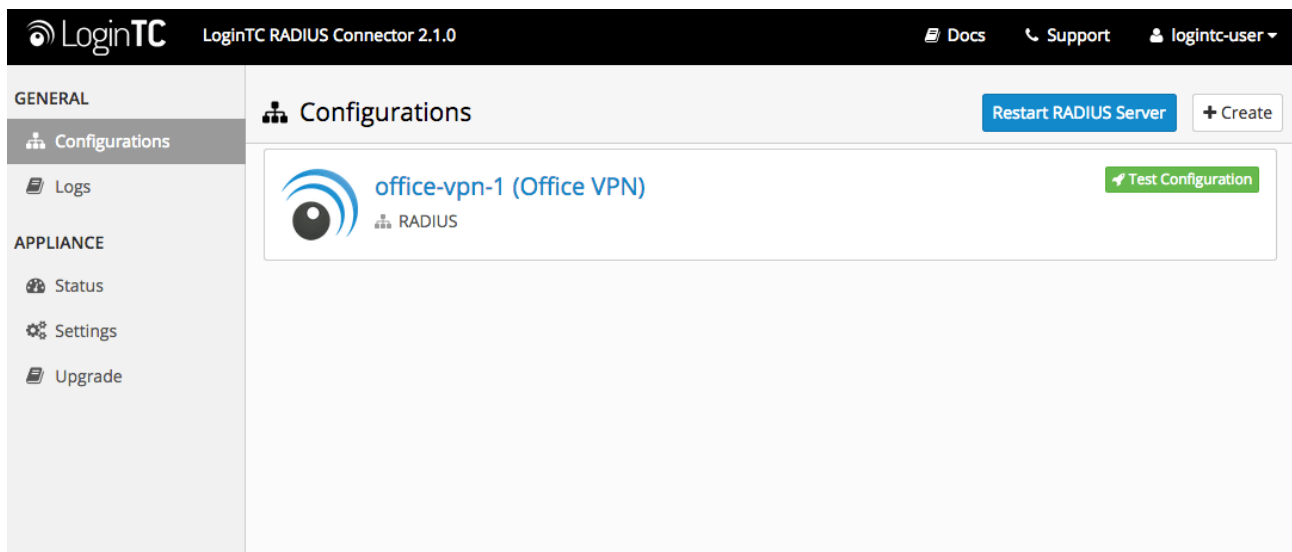
Click **Test Configuration**:
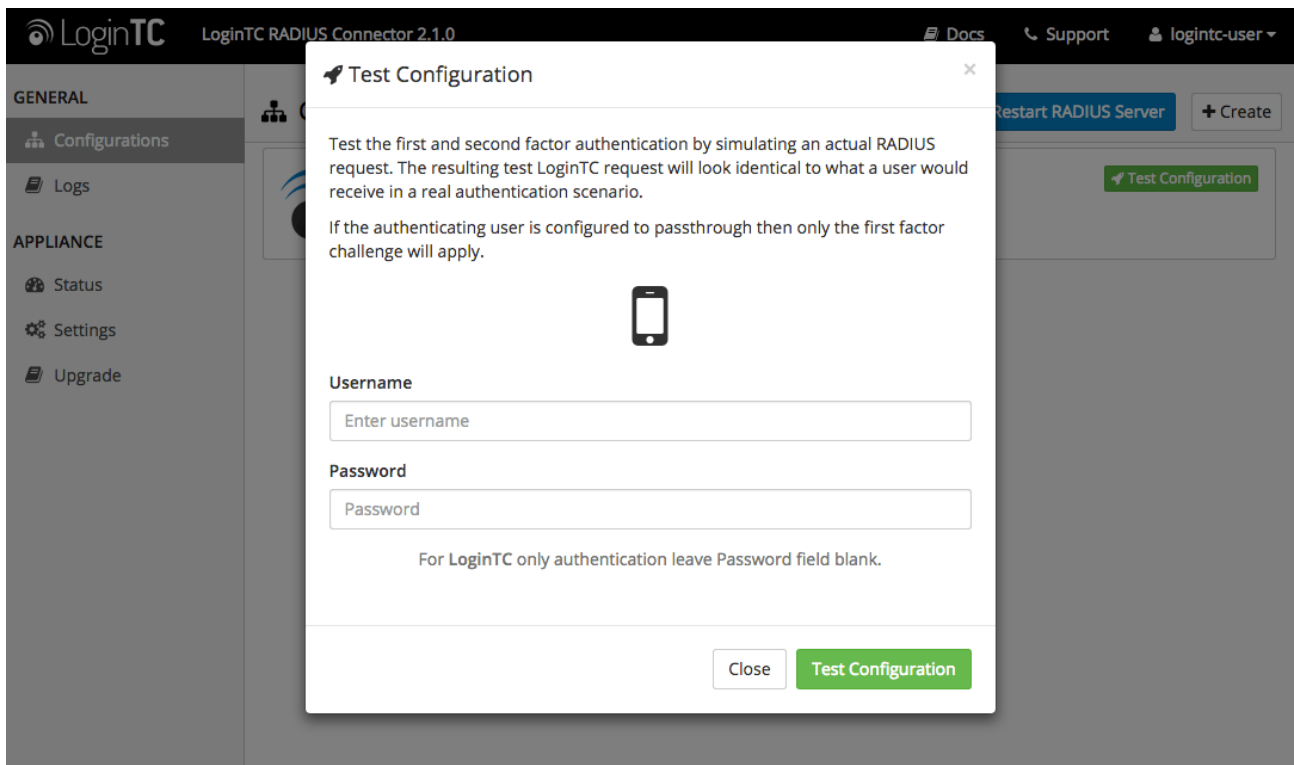
Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:
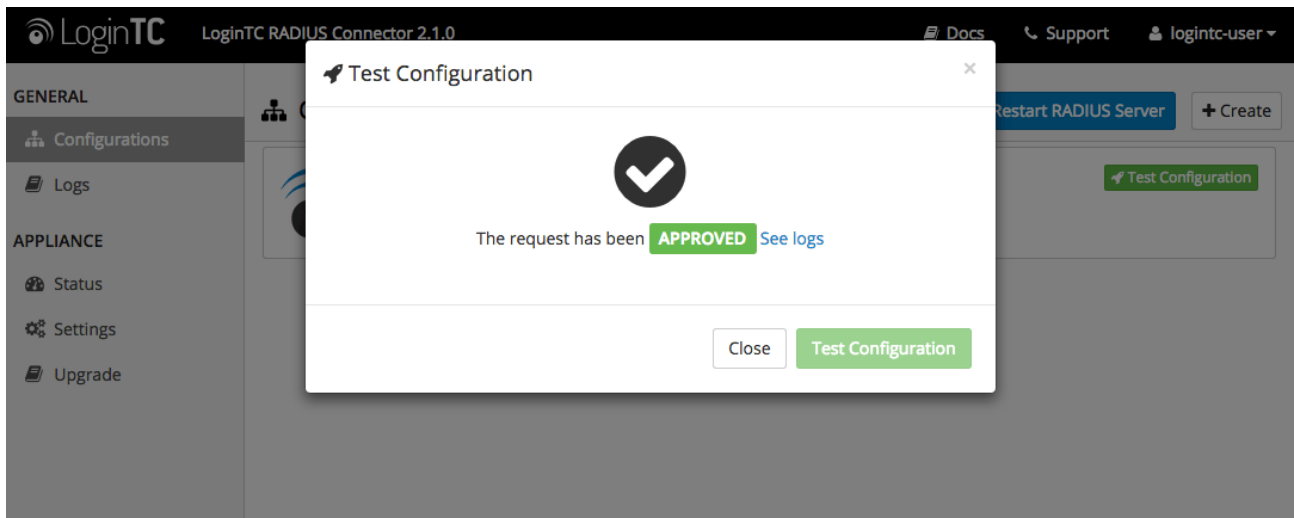
Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

If there was an error during testing, the following will appear:
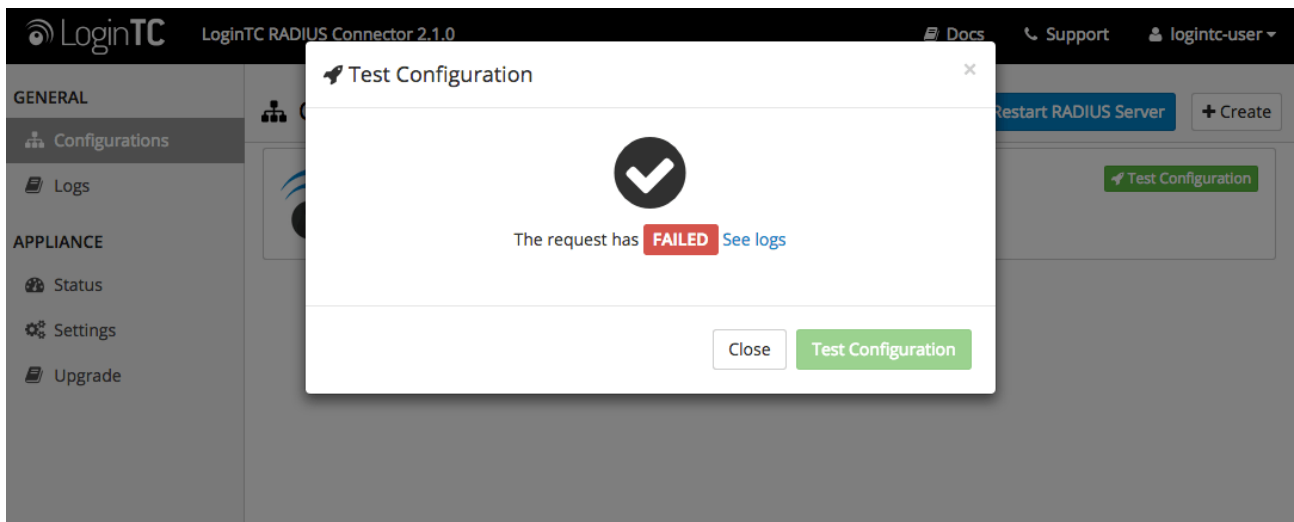
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:
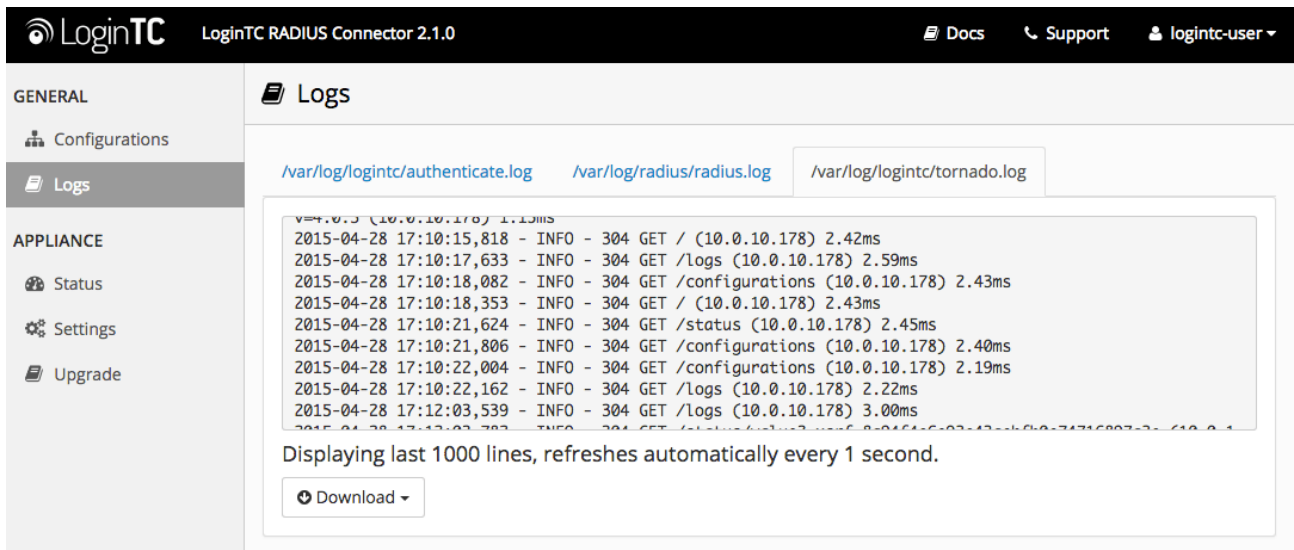
Cisco ASA Configuration - Quick Guide

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:

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**:

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

Property	Explanation	Example
Accounting Mode	Indicates how accounting messages are sent. Recommended single mode.	single mode
Reactivation Mode	Specifies the method by which failed servers are reactivated.	depleted
Dead Time	Time for which a RADIUS server is skipped over by transaction requests	10
Max Failed Attempts	Maximum number of retransmission attempts. Recommended 1.	1
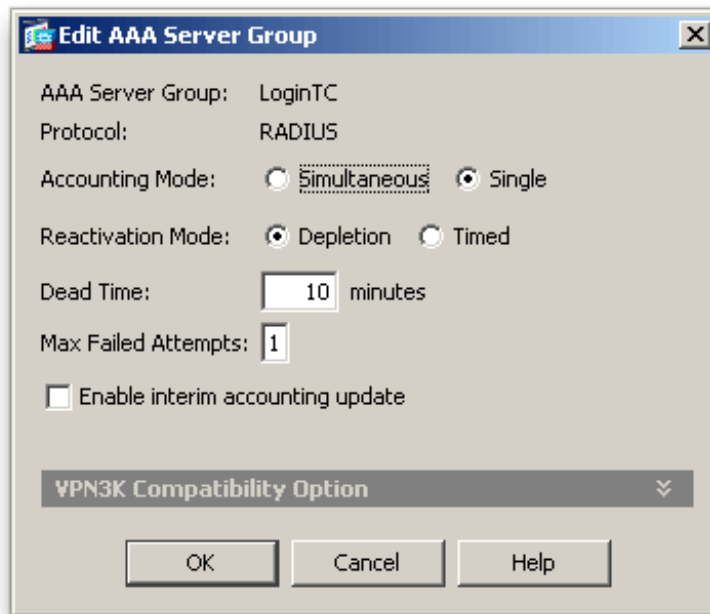
4. Select **Protocol**: RADIUS
5. Click **Add**
6. Select the newly created group
7. Under **Servers in the Selected Group** click **Add**:

Property	Explanation	Example
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. We recommend 70 seconds if you set the LoginTC Request timeout to 60 seconds.	70
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
Microsoft CHAPv2 Capable	Whether or not the RADIUS server uses CHAPv2. **Must be unchecked**	

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

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 sucessfully 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**.

Troubleshooting

User Receives Multiple LoginTC Requests

See the Knowledge Base article for more information: My Cisco ASA AnyConnect SSL VPN users receive multiple LoginTC requests. What can I do?

Time 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.

See the Knowledge Base article for more information: My Cisco ASA AnyConnect SSL VPN users receive multiple LoginTC requests. What can I do?

Not Authenticating

If you are unable to authenticate, navigate to your appliance **web interface** URL and click **Status**:
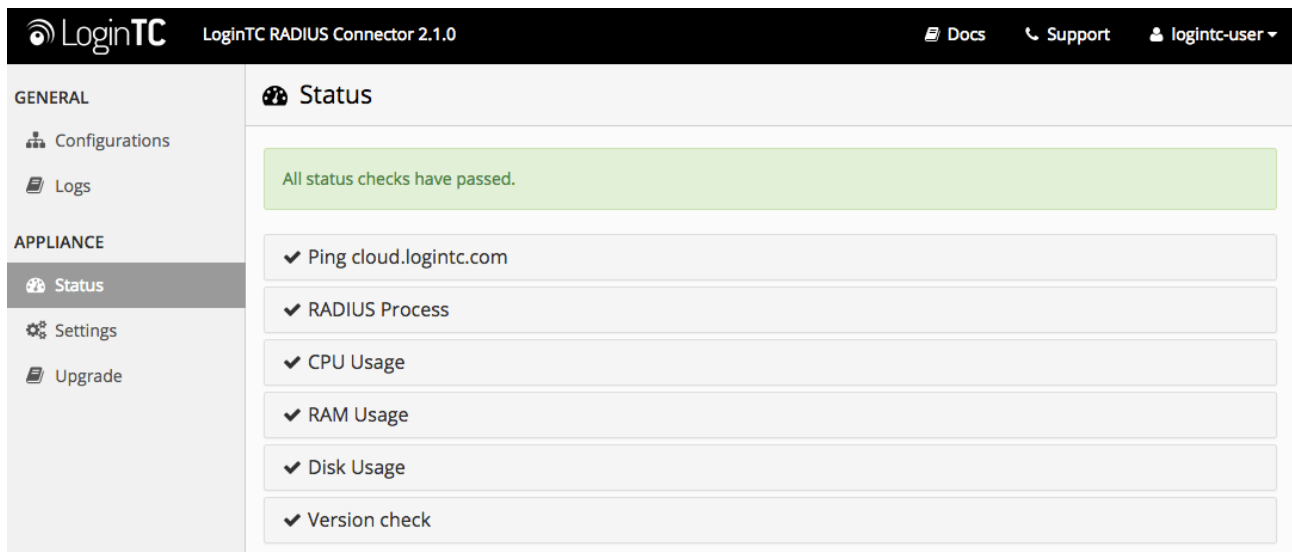
Ensure that all the status checks pass. For additional troubleshooting, click **Logs**:

Email Support

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