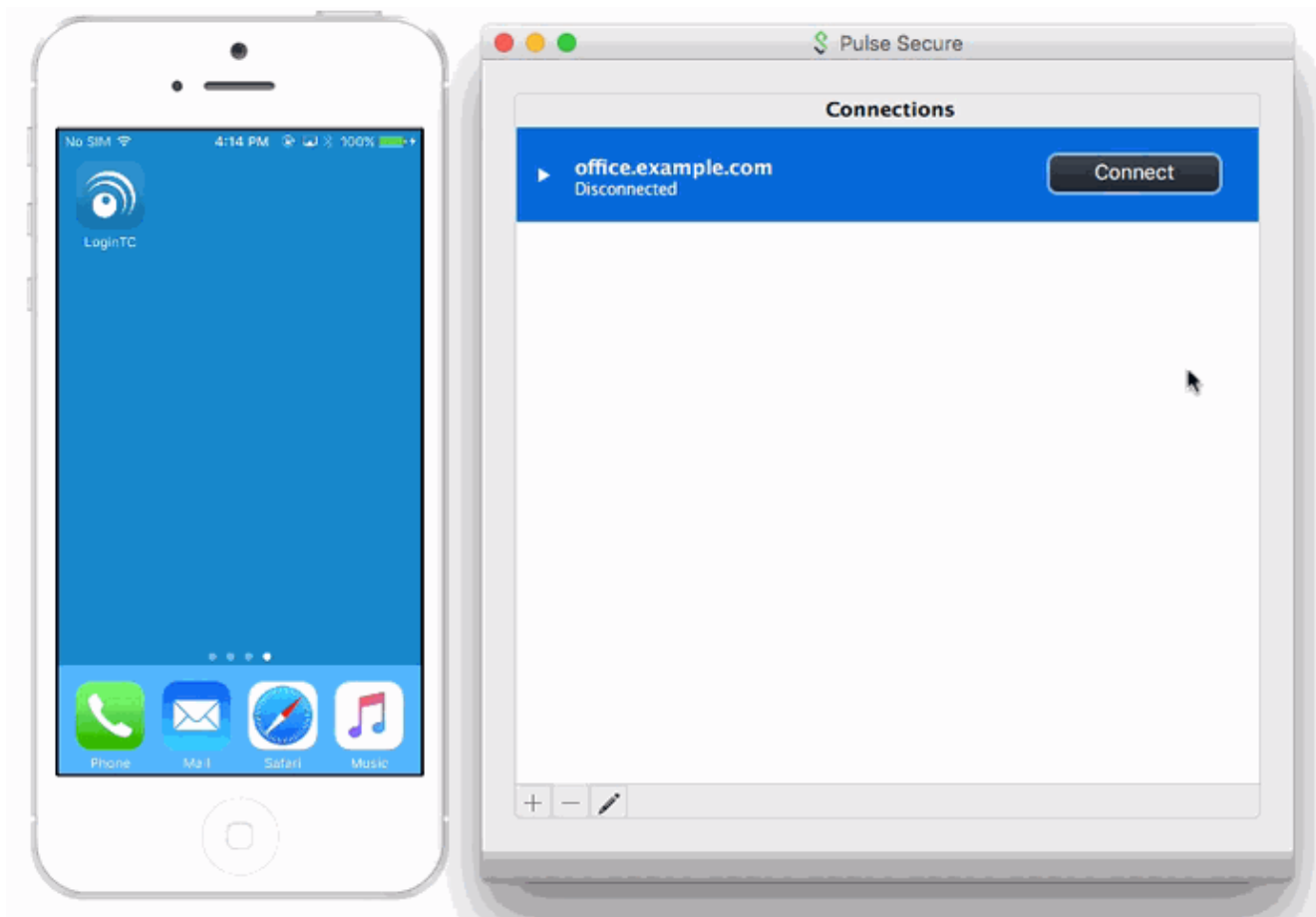


# Pulse Secure Two-Factor Authentication (2FA)

[logintc.com/docs/connectors/pulse-connect-secure](https://logintc.com/docs/connectors/pulse-connect-secure)



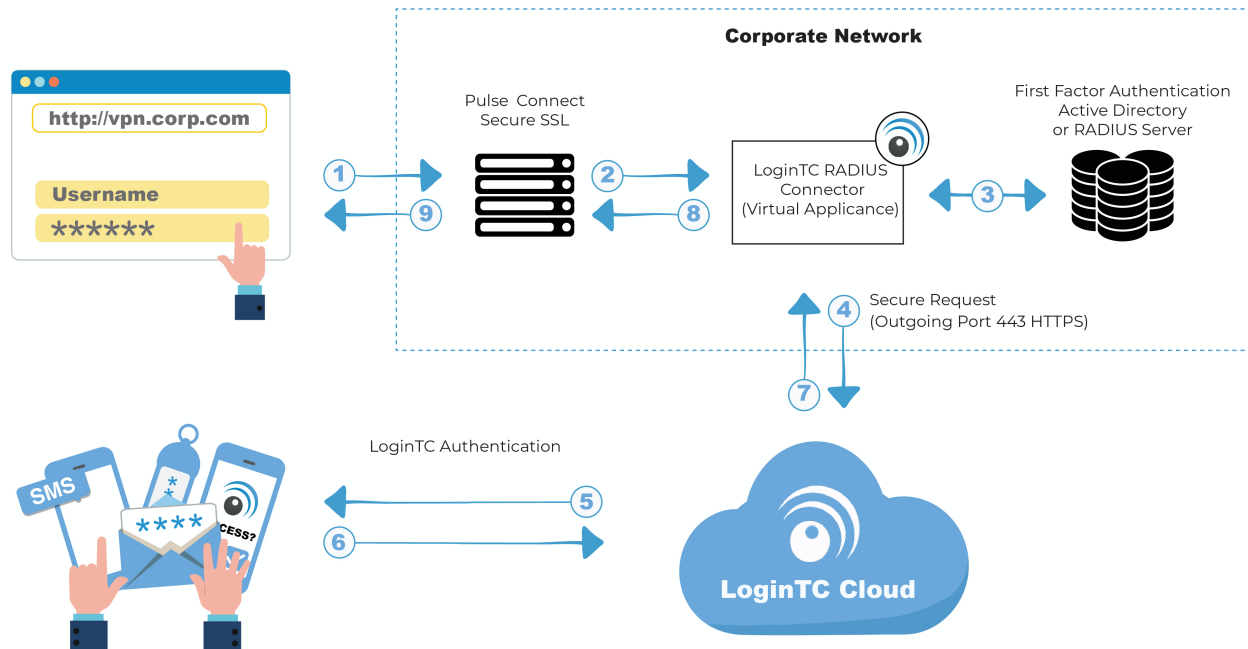
The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables Pulse Connect Secure remote access appliances to use LoginTC for the most secure two-factor authentication.

## User Experience

After entering the username and password into their VPN client, the user is presented with an Authentication Message. The user may enter '1' to receive a push notification to their device to approve or enter a valid One-Time Password (OTP). This flow works the same for clientless access.

Watch Video At: <https://youtu.be/JY5jQH842QM>

## Architecture



## Authentication Flow

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

## Compatibility

Pulse Connect Secure appliance compatibility:

Pulse Connect Secure

## Appliance not listed?

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

## Compatibility Guide

Pulse Connect Secure and any other appliance which have configurable RADIUS authentication are supported.

## Prerequisites

Before proceeding, please ensure you have the following:

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

## Create Application

Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. RDP access to your Windows infrastructure) that you want to protect with LoginTC.

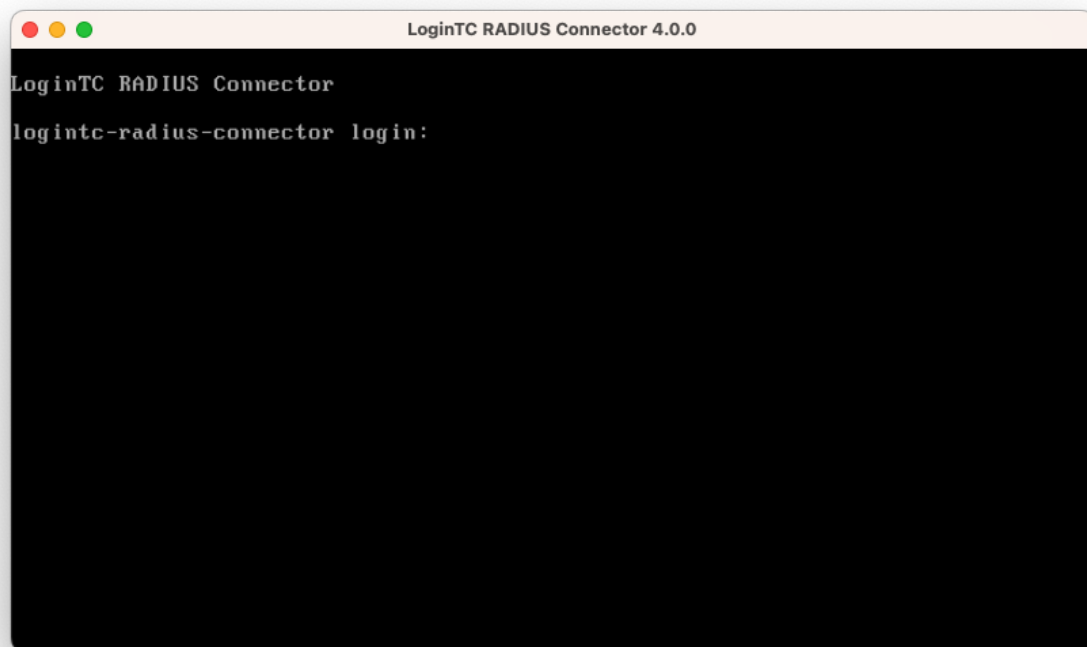
Create a LoginTC Application in [LoginTC Admin Panel](#), follow [Create Application Steps](#).

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

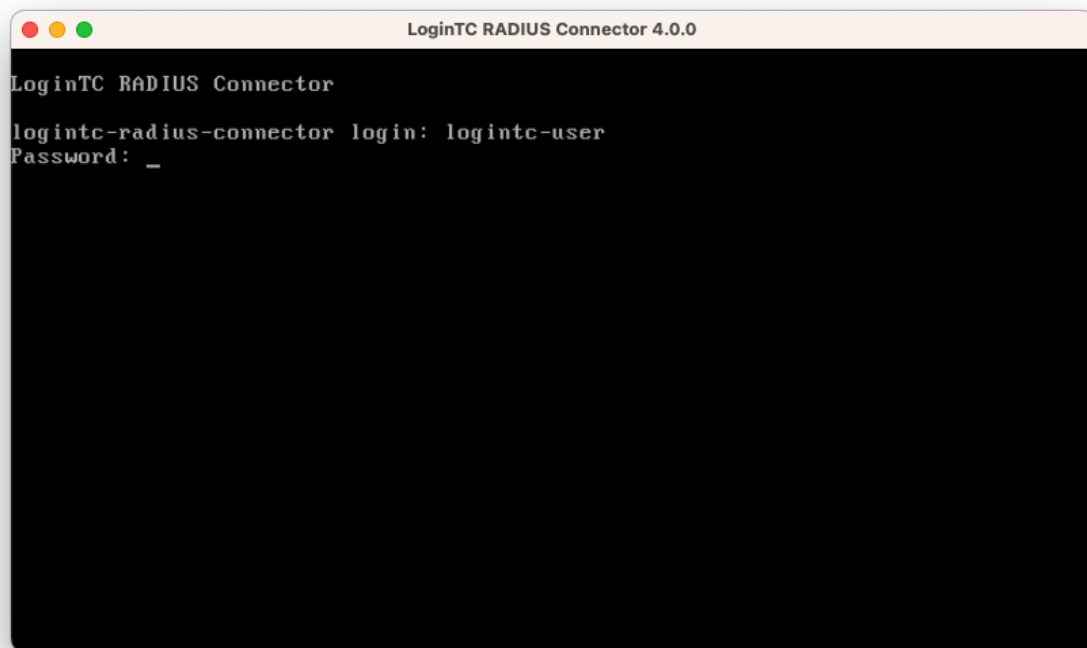
## Installation

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

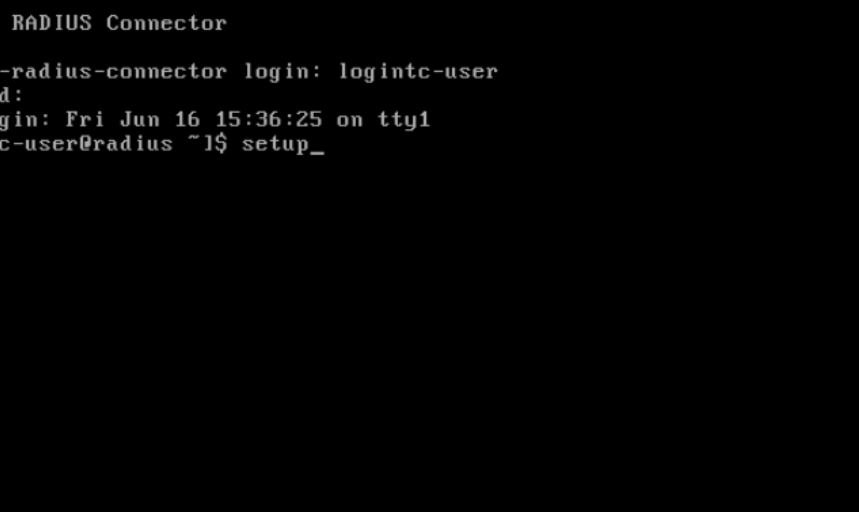
4. You will be with a console prompt:



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



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



```
LoginTC RADIUS Connector

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

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

[illegible]

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

[illegible]

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

```

LoginTC RADIUS Connector 4.0.0

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

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

Network configuration summary:

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

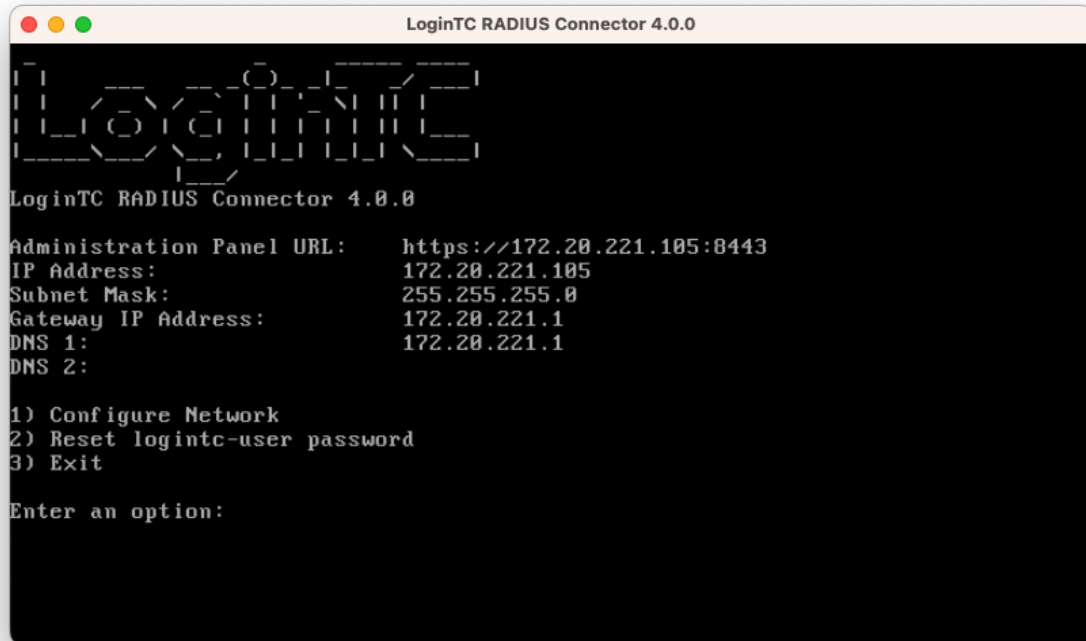
Is this correct?

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

Enter an option:

```

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



```

LoginTC RADIUS Connector 4.0.0

LoginTC
-----
LoginTC RADIUS Connector 4.0.0

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

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

Enter an option:
```

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



**LoginTC RADIUS Connector**

**Username**

**Password**

**Log in**

Version 0.1.0-SNAPSHOT



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



LoginTC RADIUS Connector

Username

logintc-user

Password

\*\*\*\*\*

Log in

Version 0.1.0-SNAPSHOT

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



Welcome to LoginTC RADIUS Connector!

Organization API Key

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

[Change LoginTC API Host](#)

HTTP Proxy ☐ Enabled ☒ Disabled

Next

[Log out](#)

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



Organization Found:

Example Inc.

Continue to LoginTC RADIUS Connector

[Log out](#)

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



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

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

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

Yes, import configurations from an existing LoginTC RADIUS Connector

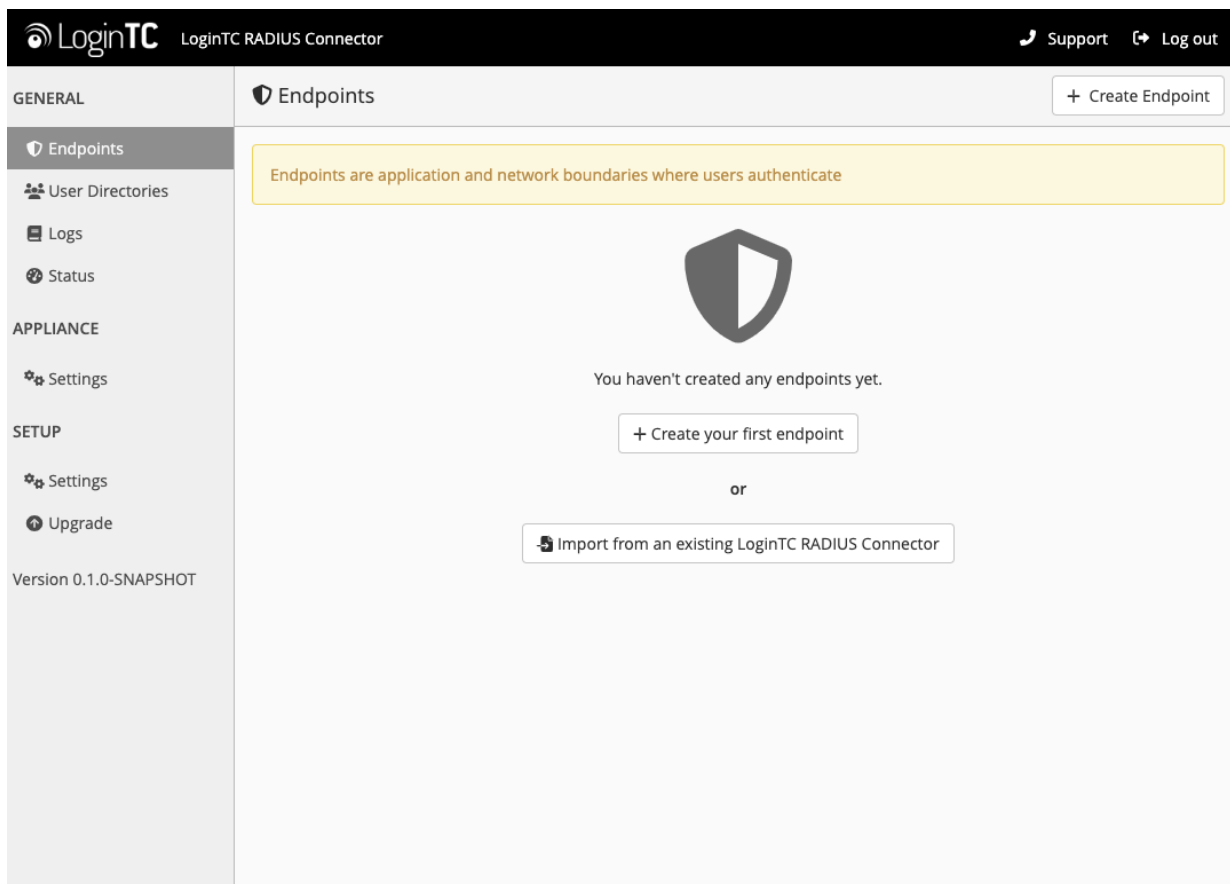
No, continue to the administration panel

[Log out](#)

#### NOTE

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

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



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

| Port | Protocol | Purpose                               |
|------|----------|---------------------------------------|
| 1812 | UDP      | RADIUS authentication                 |
| 443  | TCP      | API traffic                           |
| 8443 | TCP      | Web interface                         |
| 123  | UDP      | NTP, Clock synchronization (outgoing) |

**Note:** Username and Password `logintc-user` is used for SSH and web access. The default password is `logintcradius`. You will be asked to change the default password on first boot of the appliance.

### Configuration for Pulse Secure 2FA

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

#### 1. LoginTC Settings

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

## 2. User Directory

This section describes how the appliance will conduct an optional first factor. Either against an existing LDAP, Active Directory or RADIUS server. If no first factor is selected, then only LoginTC will be used for authentication.

## 3. Challenge Strategy / Passthrough

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

## 4. Client Settings

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

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

### First Endpoint

---

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

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

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints

Create Endpoint

Endpoints are application and network boundaries where users authenticate

You haven't created any endpoints yet.

Create your first endpoint

or

Import from an existing LoginTC RADIUS Connector

## LoginTC Settings

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

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade


Version 4.0.0

Endpoints / Create / LoginTC Application

Step 1 of 4

Cancel


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



Cisco ASA SSL VPN

Cisco ASA SSL VPN


Example Inc. Secure Access



Fortinet FortiGate SSL VPN

Fortinet FortiGate SSL VPN


Example Inc. Secure Access



Generic AD FS

Generic AD FS


Example Inc. Secure Access



Generic RADIUS

Generic RADIUS

Example Inc. Secure Access



Microsoft OWA

Configure the application:

16/54



LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints / Create / LoginTC Application

Step 1 of 4
Back
Cancel

Endpoints

User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

Generic RADIUS

Generic RADIUS
Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

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

Application API Key

79EPAK5OgrVEK1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDI24D9V1

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

Request Timeout

Request Timeout

60

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

IP Address

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

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

RADIUS Attribute Name

Calling-Station-Id

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

Test
Next

Click Test before continuing.

Configuration values:

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

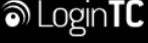
The Application ID and Application API Key are found on the [LoginTC Admin Panel](#).

## Request Timeout

17/54

Make a note of what you set the Request Timeout to as you will need to use a larger timeout value in your RADIUS client. We recommend setting the Request Timeout value to 60 seconds in the LoginTC RADIUS Connector and setting the RADIUS authentication server timeout to 70 seconds in RADIUS Client. For more information see: [Recommended settings for an optimal user experience for VPN access](#)

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

 LoginTC RADIUS Connector

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

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP


Settings

Upgrade

Version 4.0.0

Endpoints / Create / LoginTC Application

Step 1 of 4 Back Cancel

 Generic RADIUS

Generic RADIUS

Generic RADIUS Example Inc. Secure Access

LoginTC Application

Application ID

3682ec813e2fd280032ad0cf57ec140923405391

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

Application API Key

79EPAK5OgrVEk1p5D3po4n7mtCD23JdAqaAGPKLKcPHsLMHne2KRrDvdDI24D9V1

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

Request Timeout

Request Timeout

60

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

IP Address

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

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

☐ No, do not send IP Address of originating request

RADIUS Attribute Name

Calling-Station-Id


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



Test Next

Test successful, click Next to continue.

## User Directory

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

 LoginTC RADIUS Connector

 Support  Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings


Upgrade


Version 4.0.0


Endpoints / Create / User Directory

Step 2 of 4 Back Cancel


Select a user directory to leverage for username and password authentication

 **Active Directory**  
Leverage your Active Directory.

 **Generic LDAP**  
Leverage your LDAP server.

 **Generic RADIUS**  
Leverage your RADIUS server.

or

 **Continue without a User Directory**  
Users will not be challenged with password authentication. (Can be changed at any time)

## Active Directory / Generic LDAP Option

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

19/54

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

User Directories / Create / Configure Active Directory Server

Step 2 of 2
Back
Cancel

Connection Details

Name (optional)

Active Directory Server

Name of the Active Directory server.

IP Address or Host Name

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

Port (optional)

389

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

☒ No connection encryption
☐ SSL
☐ STARTTLS

Bind Details

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

☒ Bind with credentials
☐ Anonymous

Bind DN

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

Bind Password

The password for the above Bind DN account.

Query Details

Where and how to find relevant user entries.

Base DN

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

Configuration values:

| Property        | Explanation   | Examples                         |
|-----------------|---|----------------------------------|
| host            | Host or IP address of the LDAP server                 | ldap.example.com or 192.168.1.42 |
| port (optional) | Port if LDAP server uses non-standard (i.e., 389/636) | 4000                             |
| bind_dn         | DN of a user with read access to the directory        | cn=admin,dc=example,dc=com       |
| bind_password   | The password for the above bind_dn account            | password                         |
| base_dn         | The top-level DN that you wish to query from          | dc=example,dc=com                |


20/54

| Property                           | Explanation  | Examples  |
|------------------------------------|--|---|
| <code>attr_username</code>         | The attribute containing the user's username                             | <code>sAMAccountName</code> or <code>uid</code> |
| <code>attr_name</code>             | The attribute containing the user's real name                            | <code>displayName</code> or <code>cn</code>     |
| <code>attr_email</code>            | The attribute containing the user's email address                        | <code>mail</code> or <code>email</code>         |
| LDAP Group (optional)              | The name of the LDAP group to be sent back to the authenticating server. | <code>SSLVPN-Users</code>                       |
| <code>encryption</code> (optional) | Encryption mechanism   | <code>ssl</code> or <code>startTLS</code>       |
| <code>cacert</code> (optional)     | CA certificate file (PEM format)   | <code>/opt/logintc/cacert.pem</code>            |

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

## Existing RADIUS Server Option

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

 LoginTC RADIUS Connector
 Support Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

User Directories / Create / Configure RADIUS Server

Step 2 of 2 Back Cancel

RADIUS Server Details

Name (optional)

Generic RADIUS Server

Name of the RADIUS server.

IP Address or Host Name

The IP address or host name of the RADIUS Server.

Authentication Port

1812

The authentication port of the RADIUS server.

Shared Secret

The RADIUS shared secret.

Test Create

Click Test before continuing.

Configuration values:

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

## RADIUS Vendor-Specific Attributes

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

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

## Challenge Strategy / Passthrough

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

The screenshot shows the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the text "LoginTC RADIUS Connector", and links for "Support" and "Log out". The left sidebar contains a menu with "GENERAL" (selected), "Endpoints", "User Directories", "Logs", "Status", "APPLIANCE" (with "Settings"), and "SETUP" (with "Settings" and "Upgrade"). The main content area is titled "Endpoints / Create / Challenge Strategy" and shows "Step 3 of 4". It includes "Back" and "Cancel" buttons. A yellow instruction box states: "Select which users should be challenges with LoginTC and which should bypass LoginTC". Three options are listed: 1. "Challenge All Users" (marked with a checkmark icon) with the description "All users will be challenged with LoginTC." 2. "Challenge Users Based on Static Username List" (marked with a document icon) with the description "Only users in a static username list will be challenged with LoginTC." 3. "Challenge Users Based on Group Membership" (marked with a group of people icon) with the description "Leverage Active Directory and LDAP Group Membership to determine which users are challenges with LoginTC and which users bypass LoginTC."

For example, with smaller or proof of concept deployments select the Static List option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured First Authentication Factor. That means you will be able to

test LoginTC without affecting existing users accessing your VPN.

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

## Challenge All Users

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

## Challenge Users Based on Static Username List

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

The screenshot shows the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, 'LoginTC RADIUS Connector', and links for 'Support' and 'Log out'. The main content area is titled 'Endpoints / Create / Challenge Strategy' and indicates 'Step 3 of 4'. The left sidebar contains a menu with 'GENERAL', 'Endpoints', 'User Directories', 'Logs', 'Status', 'APPLIANCE', 'Settings', 'SETUP', 'Settings', and 'Upgrade'. The 'Endpoints' section is active, showing a 'Static Username List' configuration. The 'Challenge Users' section contains a text area for entering a newline-separated list of usernames. Below the text area, there is a 'Test' button and a 'Next' button. A yellow warning box at the bottom states 'Click Test before continuing.'

Static Username List

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

Challenge Users

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

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

Test Next

Click Test before continuing.

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

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

## Challenge Users Based on Group Membership

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

The screenshot shows the 'Create / Challenge Strategy' page in the LoginTC RADIUS Connector. The left sidebar contains navigation links: GENERAL, Endpoints, User Directories, Logs, Status, APPLIANCE, Settings, SETUP, Settings, Upgrade, and Version 4.0.0. The main content area is titled 'Group Membership' and includes a note: 'Precedence is always given to bypass groups when both challenge and bypass groups are specified.' Below this are two text input fields: 'Challenge Groups' and 'Bypass Groups'. The 'Challenge Groups' field has a placeholder text: 'Comma separated list of groups whose users will be challenged with LoginTC. Example: 2FA Users'. The 'Bypass Groups' field has a placeholder text: 'Comma separated list of groups whose users will always bypass LoginTC. Example: No 2FA Users'. At the bottom, there are 'Test' and 'Next' buttons. A yellow warning box at the bottom right says 'Click Test before continuing.'

Configuration values:

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

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

## Client Settings

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



LoginTC RADIUS Connector
 Support Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade

Version 4.0.0

Endpoints / Create / Client Settings

Step 4 of 4
Back
Cancel

Generic RADIUS Details

Name (optional)

Name for the endpoint.

IP Address
+

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

Shared Secret

The RADIUS shared secret.

Authentication Mode
☒ Direct
☐ Iframe
☐ Challenge
☐ Challenge Interactive

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

Client configuration values:

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

Under Authentication Mode select **Challenge**

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade

Version 4.0.0

Endpoints / Create / Client Settings

Step 4 of 4
Back
Cancel

Generic RADIUS Details

Name (optional)

Name for the endpoint.

IP Address
+

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

Shared Secret

The RADIUS shared secret.

Authentication Mode

☐ Direct
☐ Iframe
☒ Challenge
☐ Challenge Interactive

How the LoginTC authentication is performed

The user will be prompted on how they wish to proceed with second-factor authentication (e.g. LoginTC Push, OTP, bypass code). Your RADIUS client must support RADIUS challenges to use this. Challenging the user will often result in a better user experience.

Challenge Message

The message that will appear to the user for the challenge. Note that the user must enter 1 for a LoginTC Push, or must enter an OTP or bypass code.

The user will be prompted on how they wish to proceed with second-factor authentication (e.g. LoginTC Push, OTP, bypass code). Your RADIUS client must support RADIUS challenges to use this. Challenging the user will often result in a better user experience. See [User Experience](#) for more information.

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

26/54

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints

Create Endpoint

Endpoints are application and network boundaries where users authenticate

Successfully created endpoint.

Generic RADIUS

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

## Testing

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

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

Example Inc. Business

Docs
Support
administrator@example.com

GENERAL

Domains / Example Inc. Secure Access

Dashboard

Users

Applications

Policies

Groups

Bypass Codes

Devices

Phones

Hardware Tokens

User Logs

SETUP

Domains

Administrators

Admin Logs

Create Member

Members

Settings

Members

Example Inc. Secure Access has 88 member(s)

Create Member

View Members

Attributes

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

Create Domain Attribute

Latest Actions

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

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

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

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

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

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

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

7. Open the LoginTC mobile app.

8. Enter the 10-character alphanumeric activation code:

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

No SIM 2:28 PM

Cancel Add Token Next

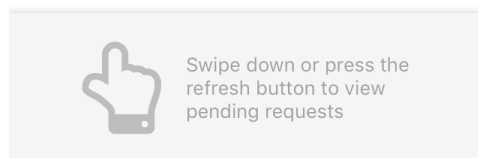
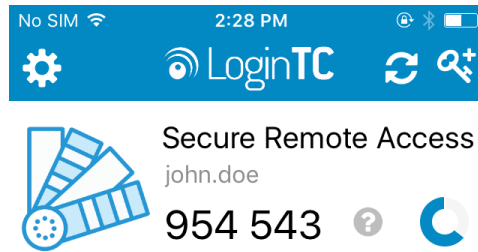
**Step 1 of 3: Enter Activation Code**

HURRMUGUVH

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

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

9. Load the token to complete the process



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

LoginTC

LoginTC RADIUS Connector

Support

Log out

GENERAL

Endpoints / Generic RADIUS

Test EndpointDelete

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Read the Generic RADIUS Documentation to integrate your Generic RADIUS application with LoginTC.

Endpoint

Endpoint NameGeneric RADIUS

Edit

LoginTC Application

Application NameGeneric RADIUS

Application ID3682ec813e2fd280032ad0cf57ec140923405391

DomainExample Inc. Secure Access

Request Timeout60

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

Edit

Click **Test Configuration**:

**Test Endpoint**

Test actual simulated request for the Endpoint. All LoginTC authentication is identical to what a user would receive in a live authentication scenario. Passthrough configuration also applies.

**Username**

**Password**

**Close** **Test Endpoint**

**LoginTC Application**

**Application Name** Generic RADIUS

**Application ID** 3682ec813e2fd280032ad0cf57ec140923405391

**Domain** Example Inc. Secure Access


**Request Timeout** 60

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

**Edit**

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:

**Test Endpoint**



The test with john.doe **APPROVED** [See logs](#)

**Try Again** **Close**

**LoginTC Application**

**Application Name** Generic RADIUS

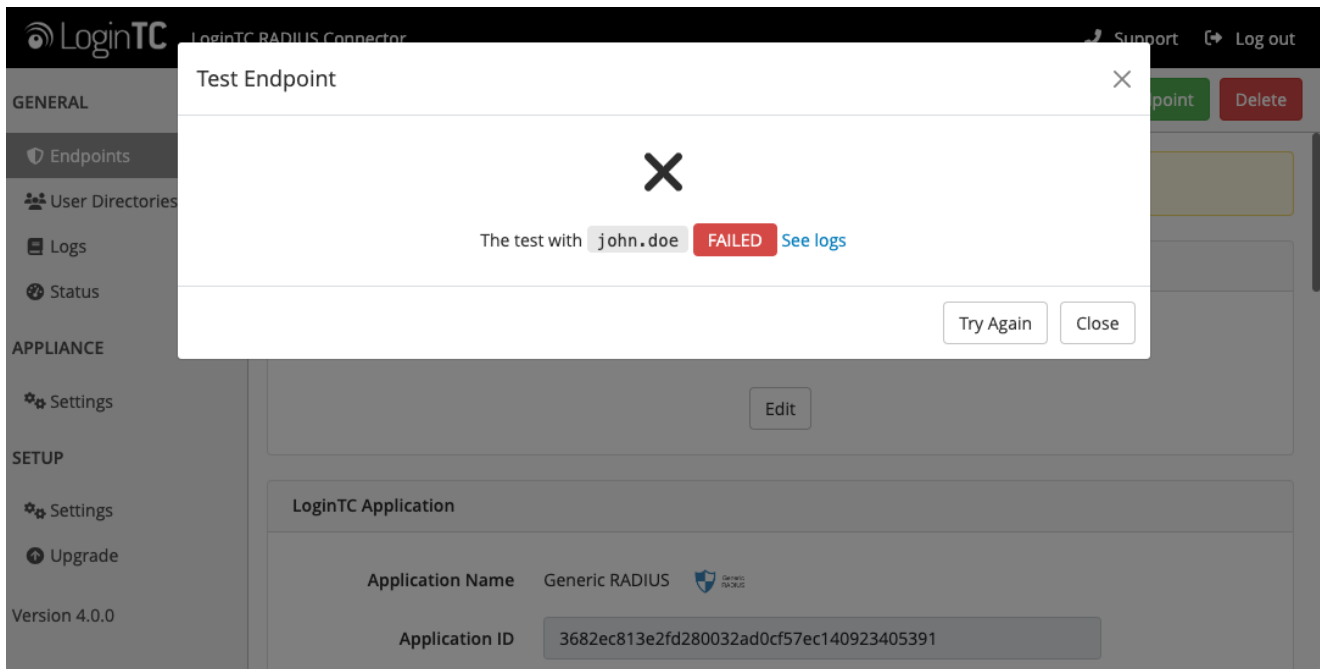
**Application ID** 3682ec813e2fd280032ad0cf57ec140923405391

**Edit**

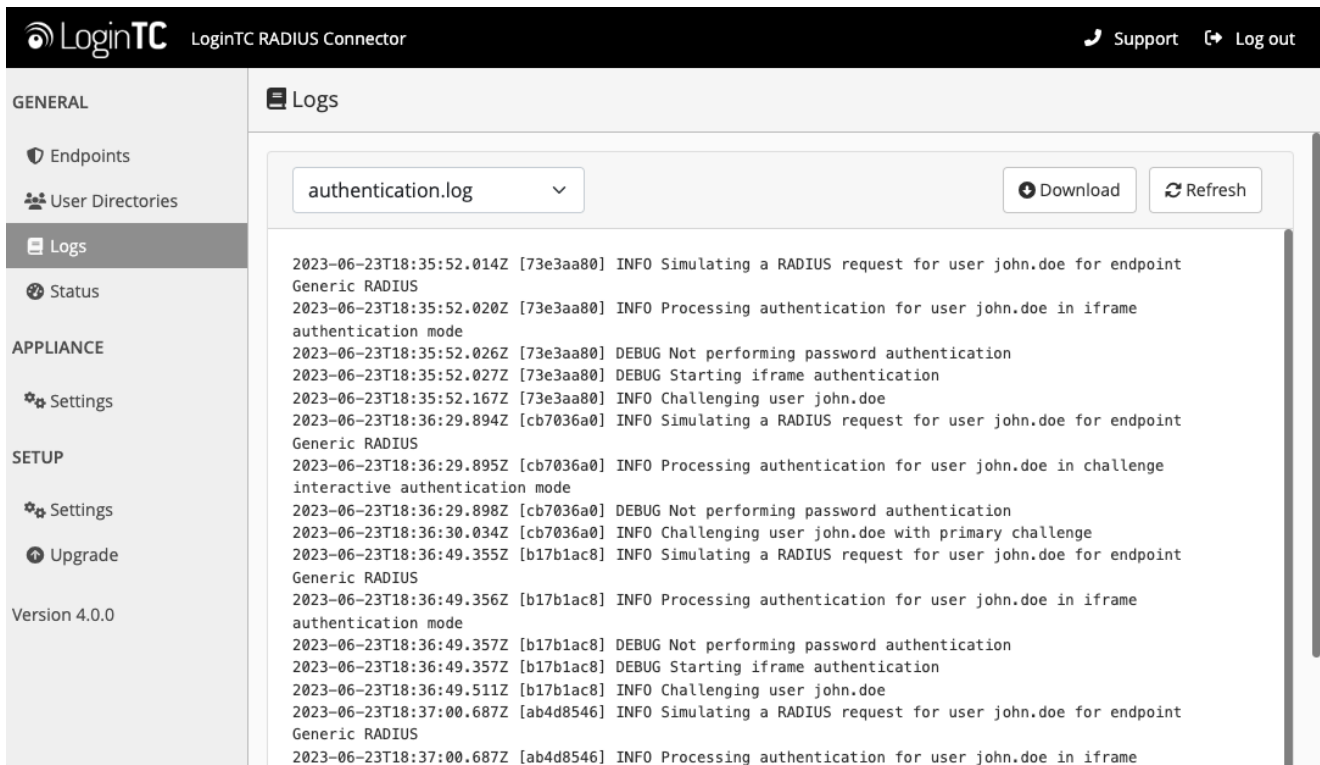


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



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



## Pulse Secure 2FA Configuration

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

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

The screenshot shows the LoginTC RADIUS Connector web interface. The top header bar is black with the LoginTC logo and 'LoginTC RADIUS Connector' on the left, and 'Support' and 'Log out' links on the right. The left sidebar is light gray and contains a menu with 'GENERAL' (Endpoints, User Directories, Logs, Status) and 'APPLIANCE' (Settings, highlighted). Below the sidebar, the main content area is titled 'Settings' with a gear icon. It contains two sections: 'RADIUS Details' and 'NTP Server'. The 'RADIUS Details' section shows 'IP Address' as 172.20.221.85 and 'RADIUS Authentication Port' as 1812. The 'NTP Server' section shows 'Enabled' with radio buttons for 'Yes' and 'No' (selected), and a message 'NTP is not enabled.' with an 'Edit' button.

| RADIUS Details             |               |
|----------------------------|---------------|
| IP Address                 | 172.20.221.85 |
| RADIUS Authentication Port | 1812          |

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

The following are quick steps to get VPN access protected with LoginTC. The instructions can be used for existing setups as well. Although these were performed on Pulse Connect Secure, the same instructions will work on other devices as well.

## Configure Pulse Connect Secure

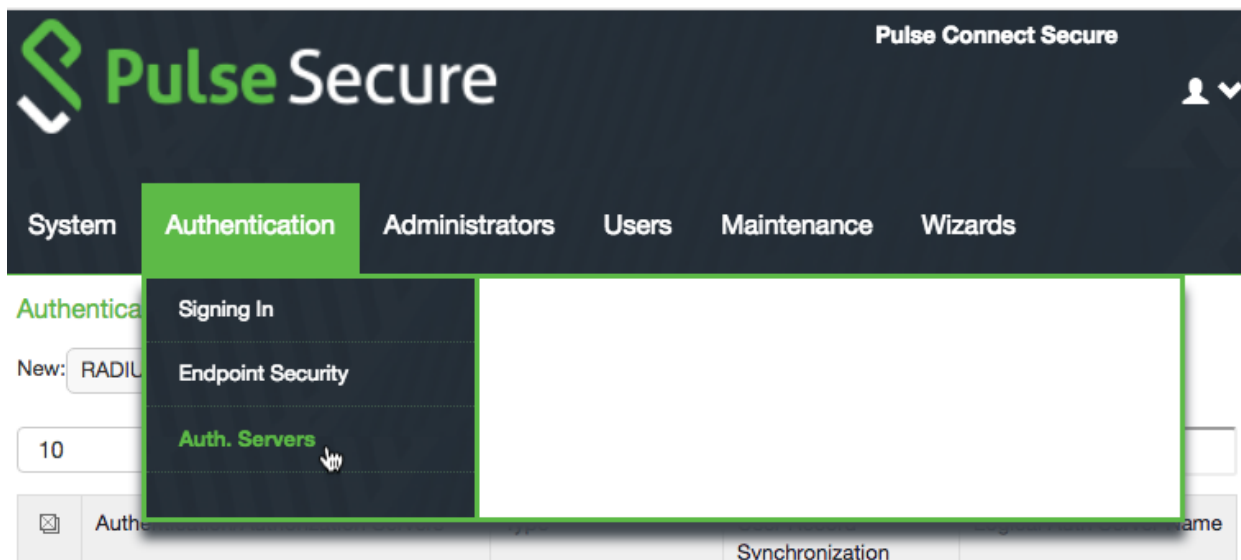
---

1. Log in to your Pulse Connect Secure (Web UI)




The image shows the Pulse Connect Secure Administrator Sign-In page. At the top, a dark blue banner contains the text "Welcome to Pulse Connect Secure" in green and white. Below the banner, the Pulse Secure logo is on the left. To the right of the logo is a sign-in form with fields for "Username" and "Password", and a green "Sign In" button. A light blue note box on the left states: "Note: This is the Administrator Sign-In Page. If you don't want to sign in as an Administrator, return to the standard Sign-In Page." Below the sign-in form, a message says: "Please sign in to begin your secure session."



2. Click **Authentication > Auth. Servers**:



3. Select **RADIUS Server** from the dropdown menu and click **New Server**:



Pulse Connect Secure



System Authentication Administrators Users Maintenance Wizards

Authentication Servers

New: 

RADIUS Server


New Server...

Delete...

10

records per page

Search:

|   |                                      |                      |                             |                          |
|---|--------------------------------------|----------------------|-----------------------------|--------------------------|
|  | Authentication/Authorization Servers | Type                 | User Record Synchronization | Logical Auth Server Name |
|   | <a href="#">Add New Server...</a>    | Local Authentication |                             |                          |

4. Complete the required fields:

**Pulse Secure** Pulse Connect Secure

System **Authentication** Administrators Users Maintenance Wizards

[Auth Servers](#) > New RADIUS Server

### New RADIUS Server

\*Name:  Label to reference this server.

NAS-Identifier:  Name of the device as known to RADIUS server

▼ **Primary Server**

\*RADIUS Server:  Name or IP address

\*Authentication Port:

\*Shared Secret:

\*Accounting Port:  Port used for RADIUS accounting, if applicable

NAS IPv4/IPv6 Address:  IPv4/IPv6 address

\*Timeout:  seconds

\*Retries:

| Property            | Explanation   | Example     |
|---------------------|---|-------------|
| Name                | The name of the Pulse Connect Secure RADIUS Server                    | LoginTC     |
| RADIUS Server       | Address of LoginTC RADIUS Connector                                   | 10.0.10.123 |
| Authentication port | RADIUS authentication port. Must be 1812.                             | 1812        |
| Shared secret       | The secret shared between the LoginTC RADIUS Connector and its client | bigsecret   |
| Accounting port     | RADIUS authentication port. Must be 1813.                             | 1813        |
| Timeout             | Amount of time in seconds to wait. At least 90s.                      | 90          |
| Retries             | Amount of times to retry authentication. Must be 0.                   | 0           |

5. Scroll down and click **Save Changes**:

---

|                        |  |  |
|------------------------|--|--|
| *Authentication Port:  | <input type="text" value="1812"/>      |  |
| *Shared Secret:        | <input type="password" value="*****"/> |  |
| *Accounting Port:      | <input type="text" value="1813"/>      | Port used for RADIUS accounting, if applicable |
| NAS IPv4/IPv6 Address: | <input type="text"/>                   | IPv4/IPv6 address                              |
| *Timeout:              | <input type="text" value="90"/>        | seconds  |
| *Retries:              | <input type="text" value="0"/>         |  |

☐ Users authenticate using tokens or one-time passwords

Note: If you select this, the device will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.

➤ Backup Server (required only if Backup server exists)


➤ RADIUS accounting

➤ Custom RADIUS Rules



➤ RADIUS Disconnect

➤ User Record Synchronization

6. Scroll down to **Custom RADIUS Rules** section and click **New RADIUS Rule...**:

 **PulseSecure**

Pulse Connect Secure

System **Authentication** Administrators Users Maintenance Wizards

Settings

Settings

Users

\*Name:

Label to reference this server.

NAS-Identifier:

Name of the device as known to RADIUS server

[➤ Primary Server](#)

[➤ Backup Server \(required only if Backup server exists\)](#)

[➤ RADIUS accounting](#)

[▼ Custom RADIUS Rules](#)

Delete

⬆

⬇

New RADIUS Rule...

| <input checked="" type="checkbox"/> | Name | Response Packet Type | Attribute criteria | Action |
|-------------------------------------|------|----------------------|--------------------|--------|
| <input type="checkbox"/>            |      |                      |                    |        |
| <input type="checkbox"/>            |      |                      |                    |        |
| <input type="checkbox"/>            |      |                      |                    |        |

7. Complete the required fields:

Auth Servers > LoginTC > Add Custom Radius Rule

Add Custom Radius Rule

Name: LoginTC RADIUS Rule

▼ If received Radius Response Packet ...

Response Packet Type: Access Challenge

Attribute criteria:

| Radius Attribute   | Operand                | Value |     |
|--------------------|------------------------|-------|-----|
| Reply-Message (18) | matches the expression |       | Add |

▼ Then take action ...

☐ show **New Pin** page

☐ show **Next Token** page

☒ show **Generic Login** page

☐ show **user login page** with error message

☐

☐ show **Reply-Message** attribute from the Radius server to the user

☐ send **Access Request** with additional attributes

| Radius Attribute | Value |  |
|------------------|-------|--|
|------------------|-------|--|

| Property             | Explanation                                   | Example                 |
|----------------------|---|-------------------------|
| Name                 | The name of the Custom RADIUS Rule            | LoginTC RADIUS Rule     |
| Response Packet Type | The type of RADIUS packet the rule applies to | Access Challenge        |
| Then take action...  | What action to take                           | show Generic Login page |

8. Scroll down and click **Save Changes**:



9. Navigate to **Users > User Realms > New User Realm**:

Pulse Secure

Pulse Connect Secure

System

Authentication

Administrators

Users

Maintenance

Wizards

Authentication Servers

New: (Select server type)

10 records per page

| <input checked="" type="checkbox"/> | Authentication/Authorization Servers | Type                 |
|-------------------------------------|--------------------------------------|----------------------|
|                                     | Administrators                       | Local Aut            |
| <input type="checkbox"/>            | LoginTC                              | RADIUS S             |
| <input type="checkbox"/>            | System Local                         | Local Authentication |

← Previous 1 Next →

User Realms

User Roles

Resource Profiles

Resource Policies

Pulse Secure Client

Enterprise Onboarding

User Realms

New User Realm

Licensed to VADTHN2MNQ1RSASIS

Copyright © 2001-2017 Pulse Secure, LLC. All rights reserved.

41/54

10. Complete the required fields:

Pulse Secure

Pulse Connect Secure

System

Authentication

Administrators

Users

Maintenance

Wizards

General

General

Authentication Policy

Role Mapping

\* Name:

LoginTC-Users

Label to reference this realm

Description:

☐ When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

LoginTC

Specify the server to use for authenticating users.

User Directory/Attribute:

Same as above

Specify the server to use for authorization.

Accounting:

None

Specify the server to use for Radius accounting.

Device Attributes:

None

Specify the server to use for device authorization.

| Property       | Explanation                         | Example       |
|----------------|-------------------------------------|---------------|
| Name           | The name of the User Realm          | LoginTC-Users |
| Authentication | The type of authentication to apply | LoginTC       |

11. Scroll down and click **Save Changes**:

[User Realms](#) > New Authentication Realm

## New Authentication Realm

\* Name:

LoginTC-Users

Label to reference this realm

Description:

☐ When editing, start on the Role Mapping page

### ▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

LoginTC

Specify the server to use for authenticating users.

User Directory/Attribute:

Same as above

Specify the server to use for authorization.

Accounting:

None

Specify the server to use for Radius accounting.

Device Attributes:

None

Specify the server to use for device authorization.

➤ [Additional Authentication Server](#)

➤ [Dynamic policy evaluation](#)

**Save Changes**

12. Navigate to **Authentication > Signing In > Sign-in Policies**:

Pulse Secure

Pulse Connect Secure

System
Authentication
Administrators
Users
Maintenance
Wizards

Signing In > S
Sign-in Po

Signing In
Endpoint Security
Auth. Servers

[Sign-in Policies](#)
[Sign-in Pages](#)
[Sign-in Notifications](#)

Sign-in SAML

[Metadata Provider](#)
[Identity Provider](#)

☐ Restrict a

Only admin
Warning: E

☐ Enable multiple user sessions

Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this check box, you limit the user to one session for all realms of this user.

☒ Display open user session[s] warning notification

Check this option to notify users if they have other active session[s] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed or cancel the login.

Select when to display a notification page to users


☒ Always
☐ If the maximum session limit per user for the realm has been reached

New URL...
Delete...
Enable
Disable


Save Changes

|                          | Administrator URLs              | Sign-In Page         | Authentication Realm(s) | Enabled                             |
|--------------------------|---------------------------------|----------------------|-------------------------|-------------------------------------|
| <input type="checkbox"/> | <a href="*/admin/">*/admin/</a> | Default Sign-In Page | Admin Users             | <input checked="" type="checkbox"/> |

13. In **User URLs** section select the URL for **Default Sign-In Page**:



Pulse Connect Secure

▼

System **Authentication** Administrators Users Maintenance Wizards

☐ Always

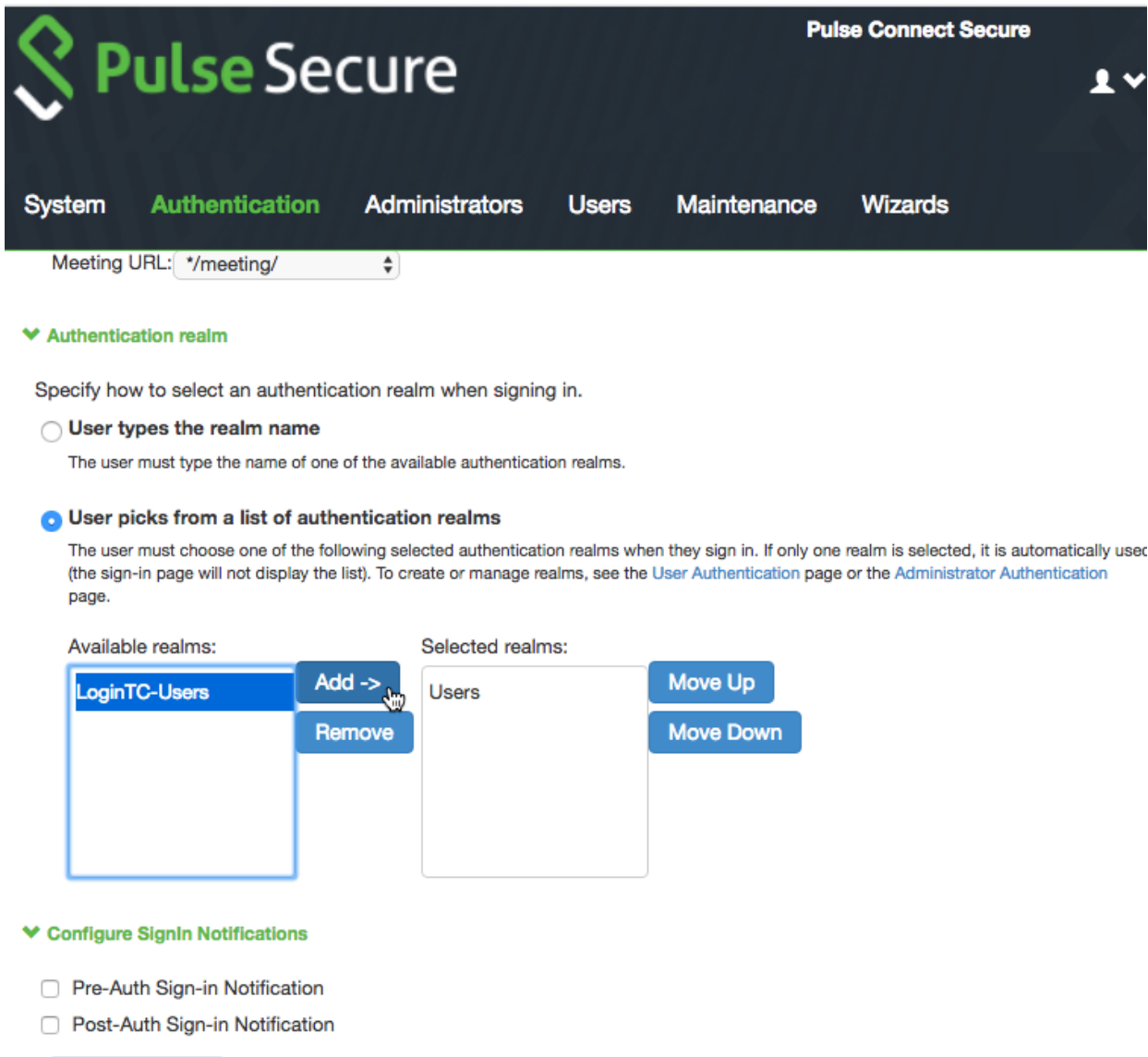
☐ If the maximum session limit per user for the realm has been reached

New URL...Delete...EnableDisable↑↓Save Changes

|                                     |                            |                      |                         |         |
|-------------------------------------|----------------------------|----------------------|-------------------------|---------|
| <input checked="" type="checkbox"/> | Administrator URLs         | Sign-In Page         | Authentication Realm(s) | Enabled |
| <input type="checkbox"/>            | <a href="#">*/admin/</a>   | Default Sign-In Page | Admin Users             | ✓       |
|                                     |                            |                      |                         |         |
| <input checked="" type="checkbox"/> | User URLs                  | Sign-In Page         | Authentication Realm(s) | Enabled |
| <input type="checkbox"/>            | <a href="#">*/</a>         | Default Sign-In Page | Users                   | ✓       |
|                                     |                            |                      |                         |         |
| <input checked="" type="checkbox"/> | Meeting URLs               | Sign-In Page         | Authentication Realm(s) | Enabled |
| <input type="checkbox"/>            | <a href="#">*/meeting/</a> | Meeting Sign-In Page |                         | ✓       |
|                                     |                            |                      |                         |         |
| <input checked="" type="checkbox"/> | Virtual Hostname           | Authorization Server | Role                    | Enabled |
|                                     |                            |                      |                         |         |

License for VAST-ING-NO-150-010

14. Under **Authentication realm** select **User picks from a list of authentication realms** and add **LoginTC-Users** from **Available realms** to **Selected realms**:



The screenshot shows the Pulse Secure web interface. At the top, the Pulse Secure logo is on the left, and "Pulse Connect Secure" is on the right. Below the logo is a navigation bar with tabs: System, Authentication (highlighted in green), Administrators, Users, Maintenance, and Wizards. Below the navigation bar is a "Meeting URL:" field with a dropdown menu showing "\*/meeting/".

Below the navigation bar, there is a section titled "Authentication realm" with a green checkmark icon. The text says: "Specify how to select an authentication realm when signing in."

There are two radio button options:

- ☐ **User types the realm name**  
The user must type the name of one of the available authentication realms.
- ☒ **User picks from a list of authentication realms**  
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Below the radio buttons, there are two columns:

- Available realms:** A list box containing "LoginTC-Users". To the right of the list box are two buttons: "Add ->" and "Remove".
- Selected realms:** A list box containing "Users". To the right of the list box are two buttons: "Move Up" and "Move Down".

Below the realms section, there is a section titled "Configure SignIn Notifications" with a green checkmark icon. It contains two checkboxes:

- ☐ Pre-Auth Sign-in Notification
- ☐ Post-Auth Sign-in Notification

There is a blue horizontal line below the checkboxes.

15. Scroll down and click **Save Changes**:

The screenshot shows the Pulse Connect Secure web interface. At the top, the logo and title 'Pulse Connect Secure' are visible. Below the navigation bar, the 'Authentication realm' section is expanded. It contains two radio button options: 'User types the realm name' (unselected) and 'User picks from a list of authentication realms' (selected). The selected option has a descriptive paragraph and links to 'User Authentication' and 'Administrator Authentication' pages. Below this, there are two columns: 'Available realms' (empty) and 'Selected realms' (containing 'Users' and 'LoginTC-Users'). Buttons for 'Add ->', 'Remove', 'Move Up', and 'Move Down' are present. At the bottom, there are checkboxes for 'Pre-Auth Sign-in Notification' and 'Post-Auth Sign-in Notification', and a 'Save Changes' button with a mouse cursor clicking it.

**Pulse Secure** Pulse Connect Secure

System **Authentication** Administrators Users Maintenance Wizards

▼ Authentication realm

Specify how to select an authentication realm when signing in.

☐ User types the realm name  
The user must type the name of one of the available authentication realms.

☒ User picks from a list of authentication realms  
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Available realms: Selected realms:

Add -> Remove Move Up Move Down

Users  
LoginTC-Users

▼ Configure SignIn Notifications

☐ Pre-Auth Sign-in Notification  
☐ Post-Auth Sign-in Notification

Save Changes

You are now ready to test your configuration.

## Testing (Pulse Connect Secure Configuration)

To test, navigate to your Pulse Connect Secure clientless VPN portal or use a Pulse Connect Secure SSL VPN client and attempt access.

## Welcome to Pulse Connect Secure

Username   
Password   
Realm

Please sign in to begin your secure session.



Sign In

### User Management

There are several options for managing your users within LoginTC:

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

### Failover

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

Edit the **Backup Server** portion of the Pulse Connect Secure RADIUS Authentication Server to configure failover:



## Settings

Settings

Users

\*Name:  Label to reference this server.

NAS-Identifier:  Name of the device as known to RADIUS server

➤ Primary Server

▼ Backup Server (required only if Backup server exists)

RADIUS Server:  Name or IP address

Authentication Port:

Shared Secret:


Accounting Port:  Port used for RADIUS accounting, if applicable

☐ Load-Balance Auth Requests between Primary and Backup Servers

Accounting requests will not be load-balanced.

## Logging

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

 LoginTC RADIUS Connector

Support Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Logs

authentication.log

Download Refresh

2023-06-23T18:35:52.014Z [73e3aa80] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS

2023-06-23T18:35:52.020Z [73e3aa80] INFO Processing authentication for user john.doe in iframe authentication mode

2023-06-23T18:35:52.026Z [73e3aa80] DEBUG Not performing password authentication

2023-06-23T18:35:52.027Z [73e3aa80] DEBUG Starting iframe authentication

2023-06-23T18:35:52.167Z [73e3aa80] INFO Challenging user john.doe

2023-06-23T18:36:29.894Z [cb7036a0] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS

2023-06-23T18:36:29.895Z [cb7036a0] INFO Processing authentication for user john.doe in challenge interactive authentication mode

2023-06-23T18:36:29.898Z [cb7036a0] DEBUG Not performing password authentication

2023-06-23T18:36:30.034Z [cb7036a0] INFO Challenging user john.doe with primary challenge

2023-06-23T18:36:49.355Z [b17b1ac8] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS

2023-06-23T18:36:49.356Z [b17b1ac8] INFO Processing authentication for user john.doe in iframe authentication mode

2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Not performing password authentication

2023-06-23T18:36:49.357Z [b17b1ac8] DEBUG Starting iframe authentication

2023-06-23T18:36:49.511Z [b17b1ac8] INFO Challenging user john.doe

2023-06-23T18:37:00.687Z [ab4d8546] INFO Simulating a RADIUS request for user john.doe for endpoint Generic RADIUS

2023-06-23T18:37:00.687Z [ab4d8546] INFO Processing authentication for user john.doe in iframe

## 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
```

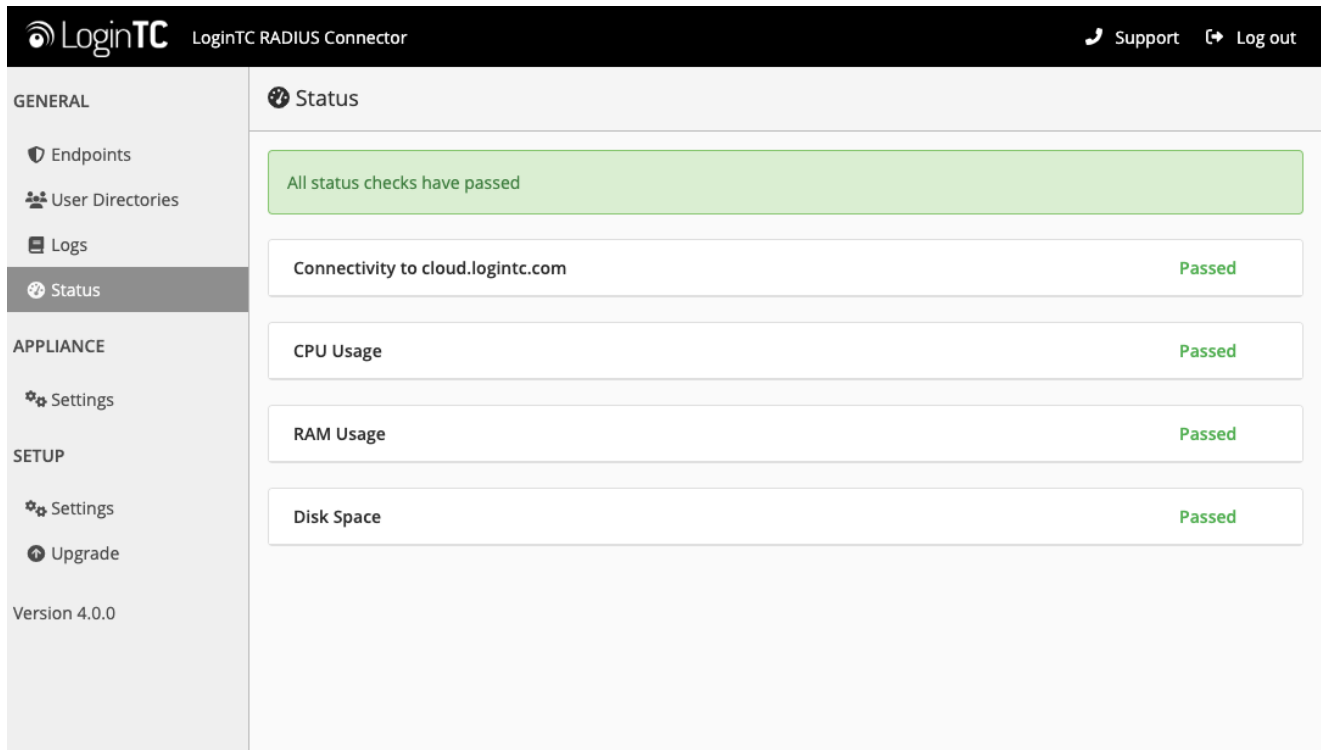
5. It's possible that the virtualization software renamed the network adapter to `eth1`. If this is the case, rename `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth1`.

```
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**:



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

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

The screenshot displays the LoginTC RADIUS Connector web interface. The top navigation bar includes the LoginTC logo, the text 'LoginTC RADIUS Connector', and links for 'Support' and 'Log out'. A left sidebar contains a menu with 'GENERAL' (selected), 'Endpoints', 'User Directories', 'Logs', 'Status', 'APPLIANCE', 'Settings', 'SETUP', 'Settings', 'Upgrade', and 'Version 4.0.0'. The main content area is titled 'Logs' and shows a dropdown menu set to 'authentication.log'. To the right of the dropdown are 'Download' and 'Refresh' buttons. The log entries are displayed in a scrollable area, showing a sequence of events for user 'john.doe' at endpoint 'Generic RADIUS', including simulation, processing, debugging, and challenging steps.

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

Unsuccessful authentication may be caused by premature [timeouts](#)

## 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.

## Email Support

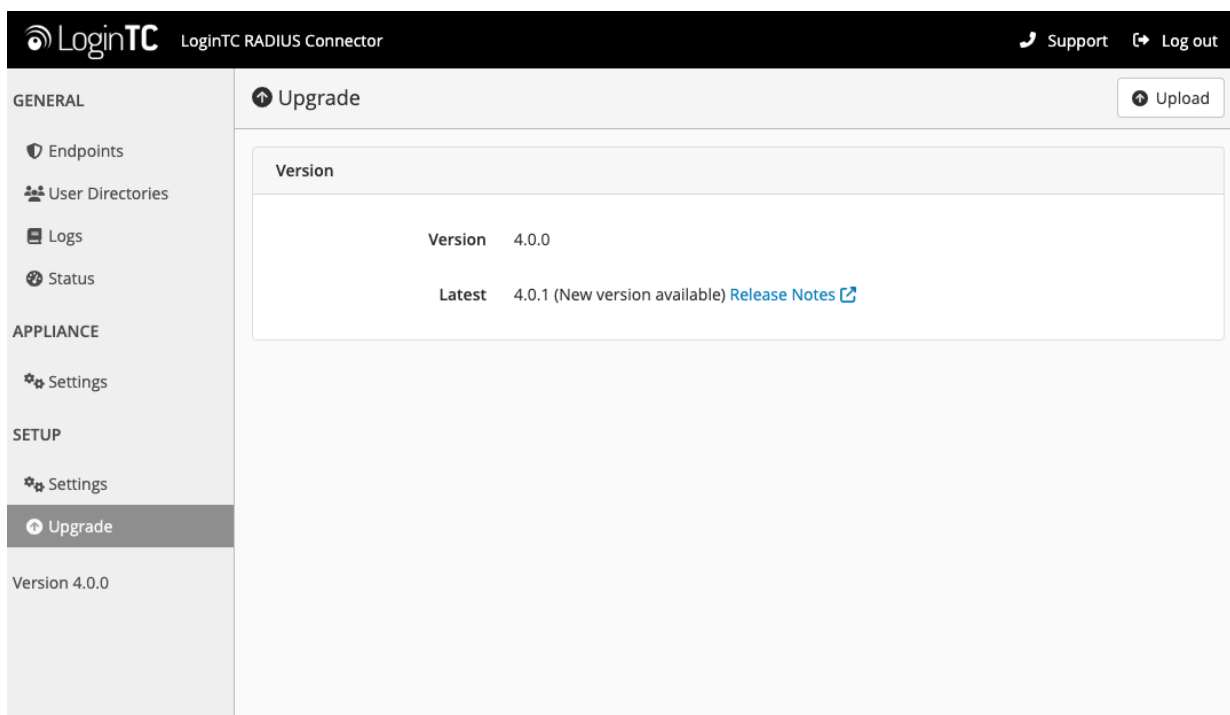
For any additional help please email [support@cyphercor.com](mailto:support@cyphercor.com). Expect a speedy reply.

## Upgrading

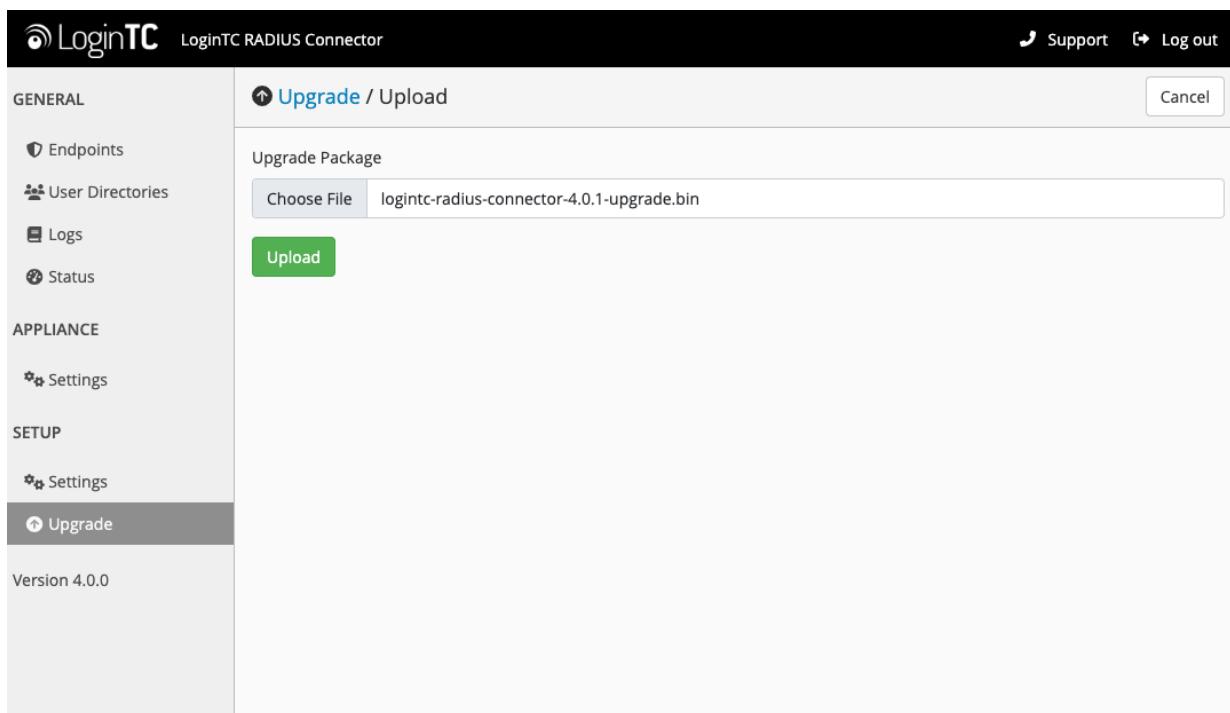
### From 4.X

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

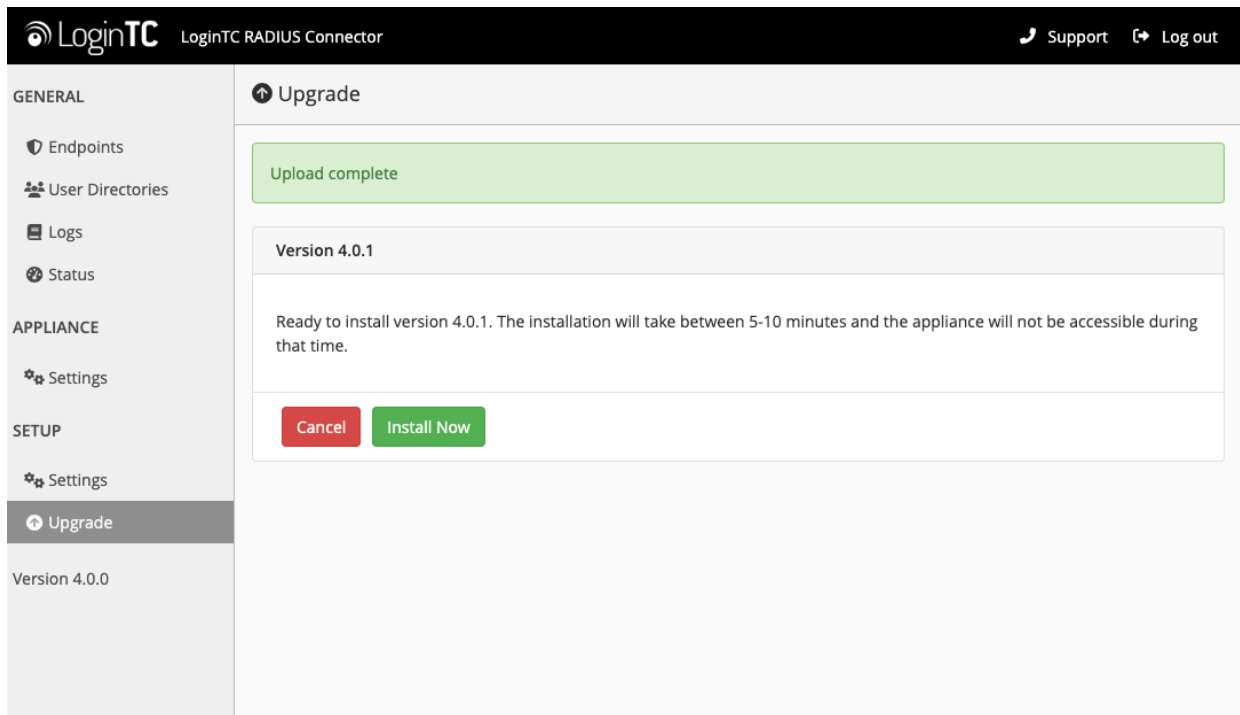
1. Navigate to **SETUP > Upgrade**:



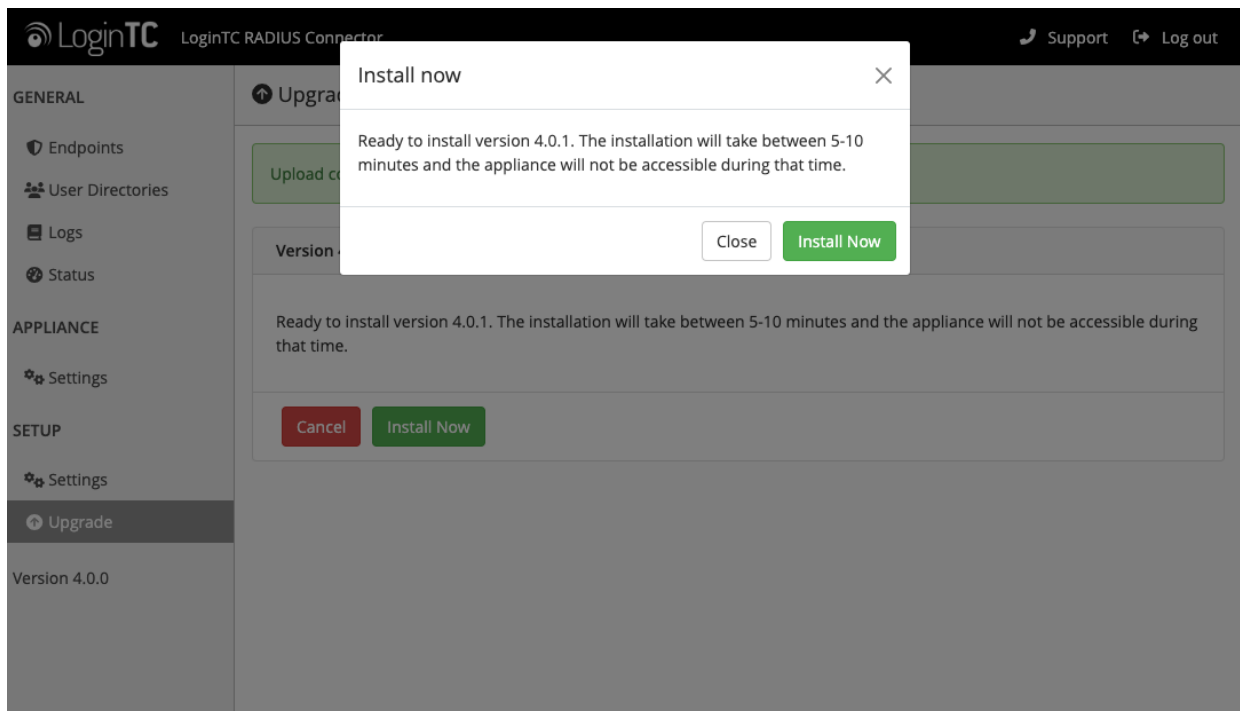
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



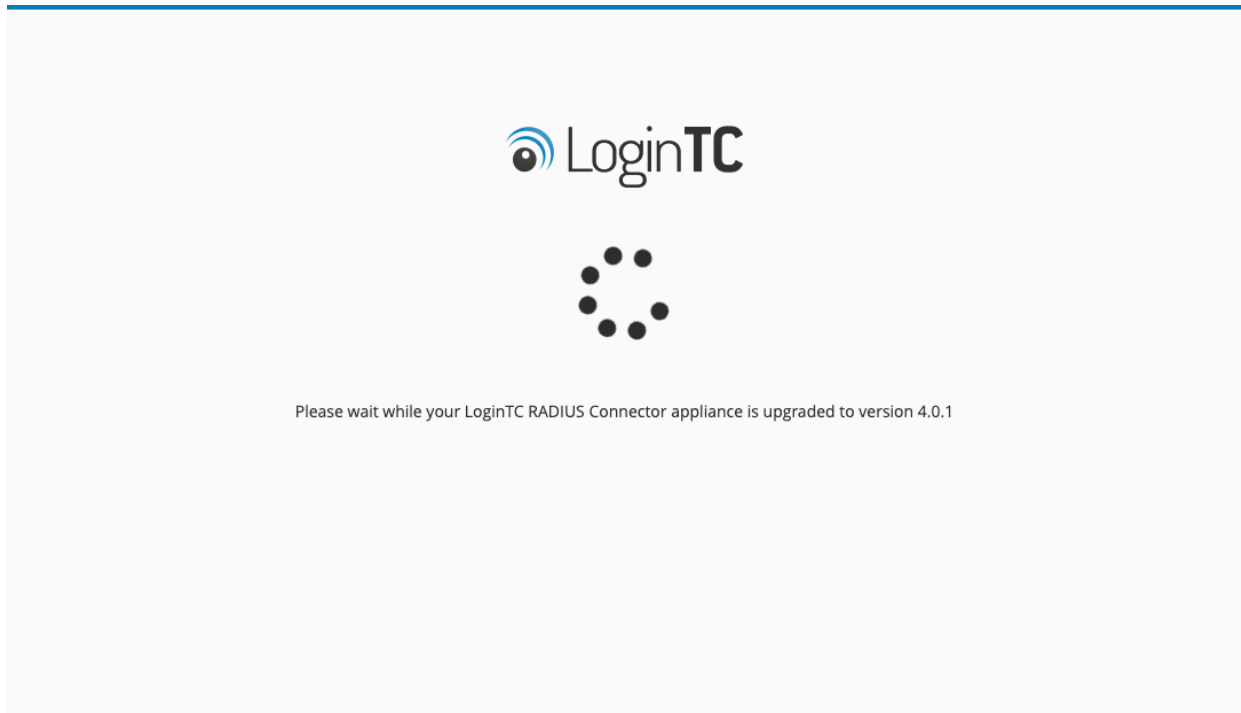
3. Click **Upload** and do not navigate away from the page:



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



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



**NOTE: Upgrade time**

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

**From 3.X**

---

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

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

**New LoginTC RADIUS Connector 4.X**

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

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