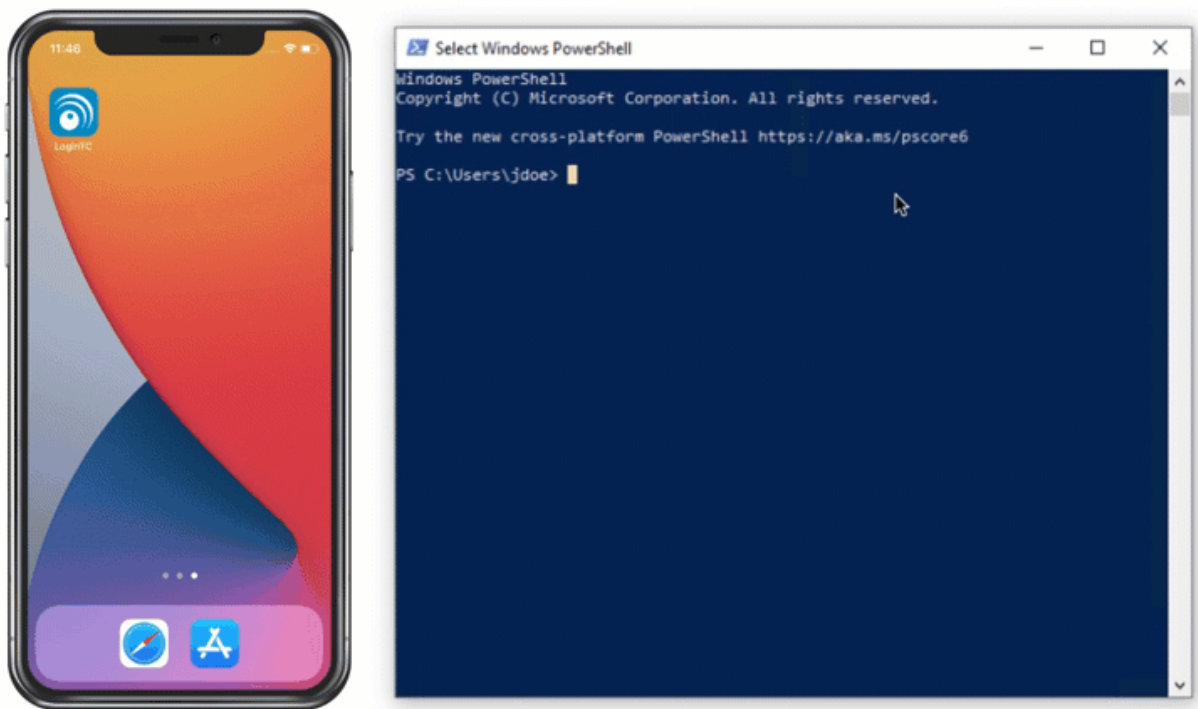


SSH Two-Factor Authentication (2FA) using PAM RADIUS module

logintc.com/docs/connectors/ssh

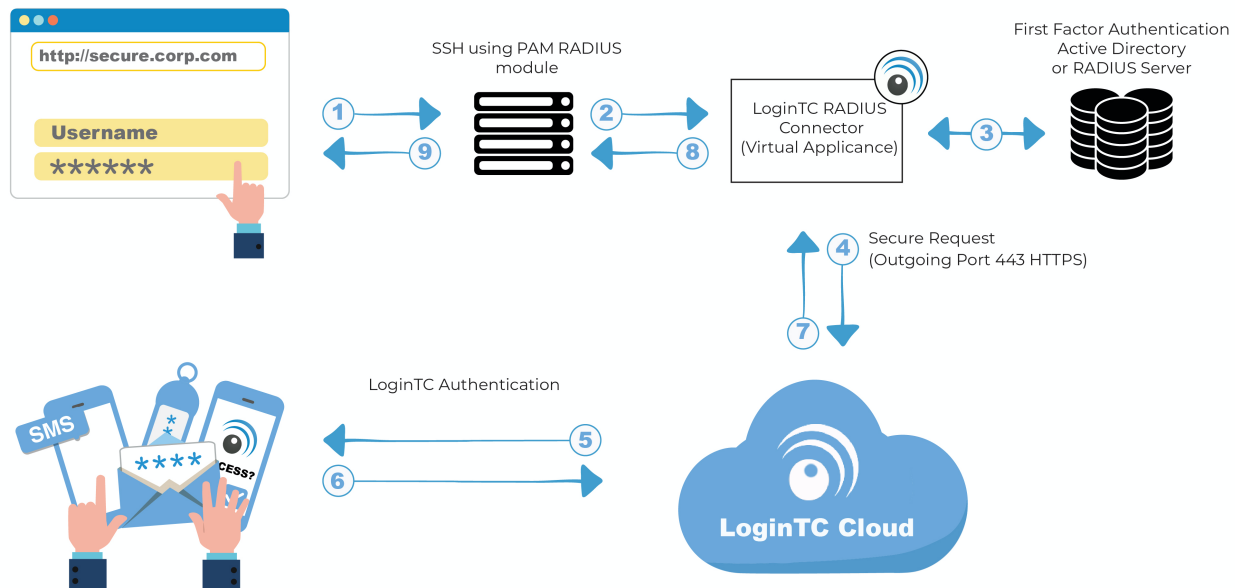


LoginTC makes it easy for administrators to add two factor authentication to SSH on their Unix systems. This document shows how to configure SSH to require two factor authentication for remote access via Pluggable Authentication Module (PAM).

User Experience

There are a wide variety of authentication mechanism users can use to perform MFA with SSH.

Architecture



Authentication Flow

1. A user attempts access 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 PAM RADIUS module
9. User is granted access via SSH

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

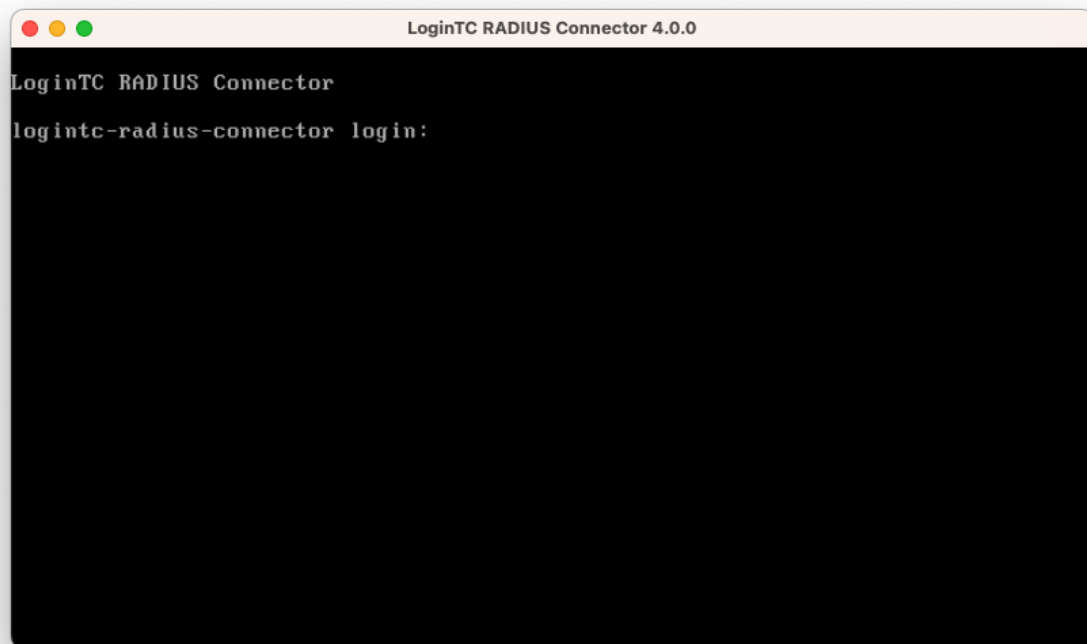
Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

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

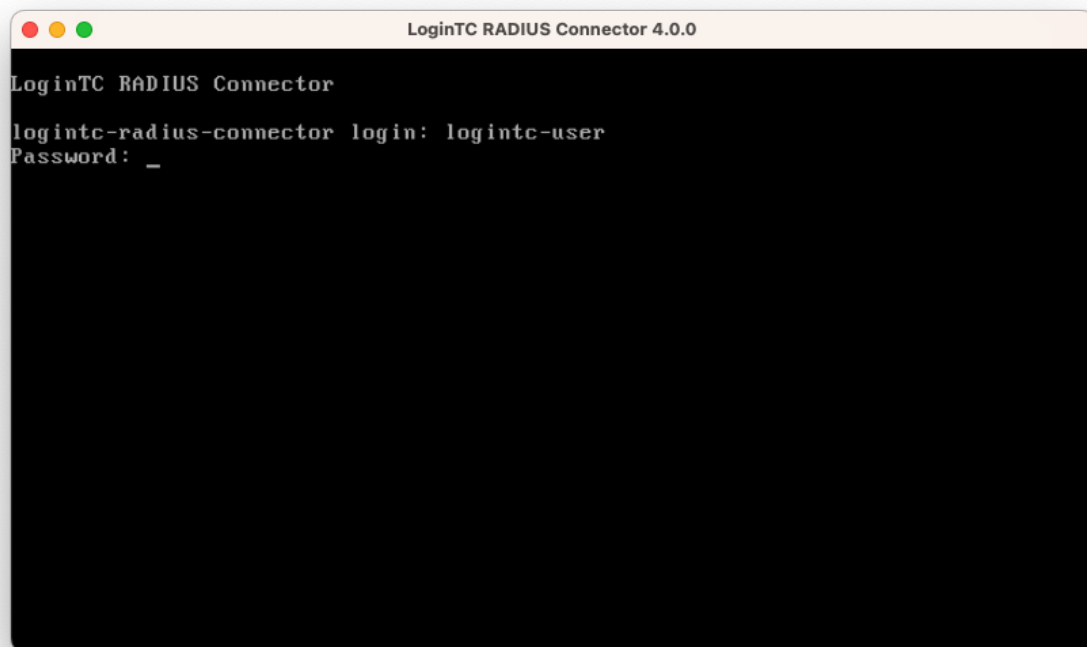
If you have already created a LoginTC Application for your deployment, then you may skip this section and proceed to [Installation](#).

Installation

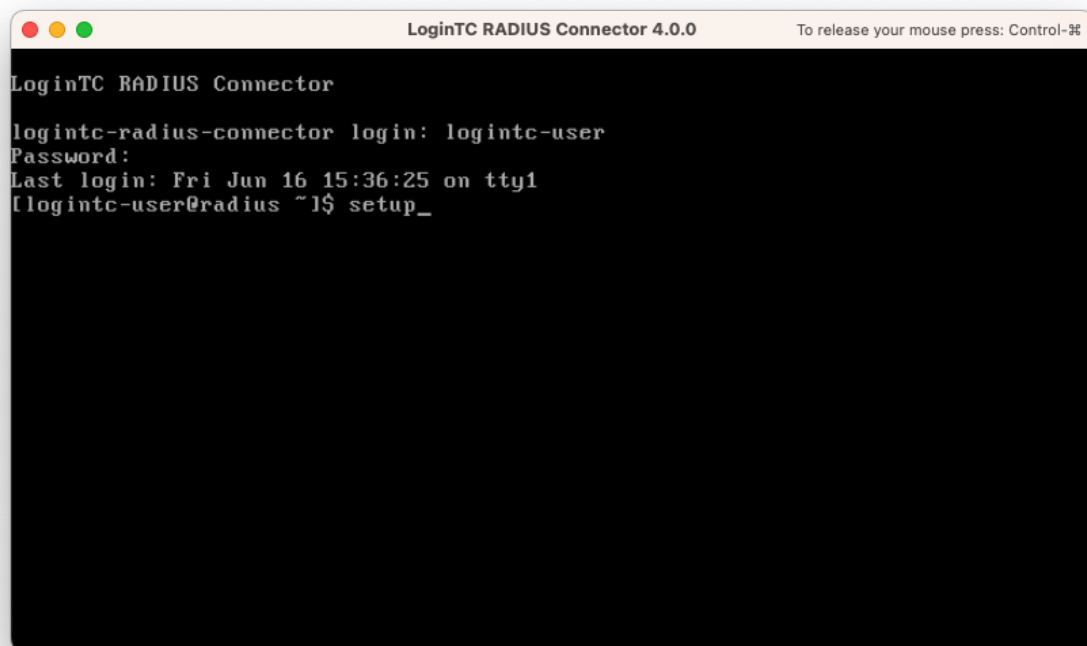
1. Import the virtual appliance your computer virtualization software
[Instructions for Hyper-V](#)
2. Ensure that LoginTC RADIUS CONNECTOR has a virtual network card
3. Start the virtual appliance
4. You will be with a console prompt:



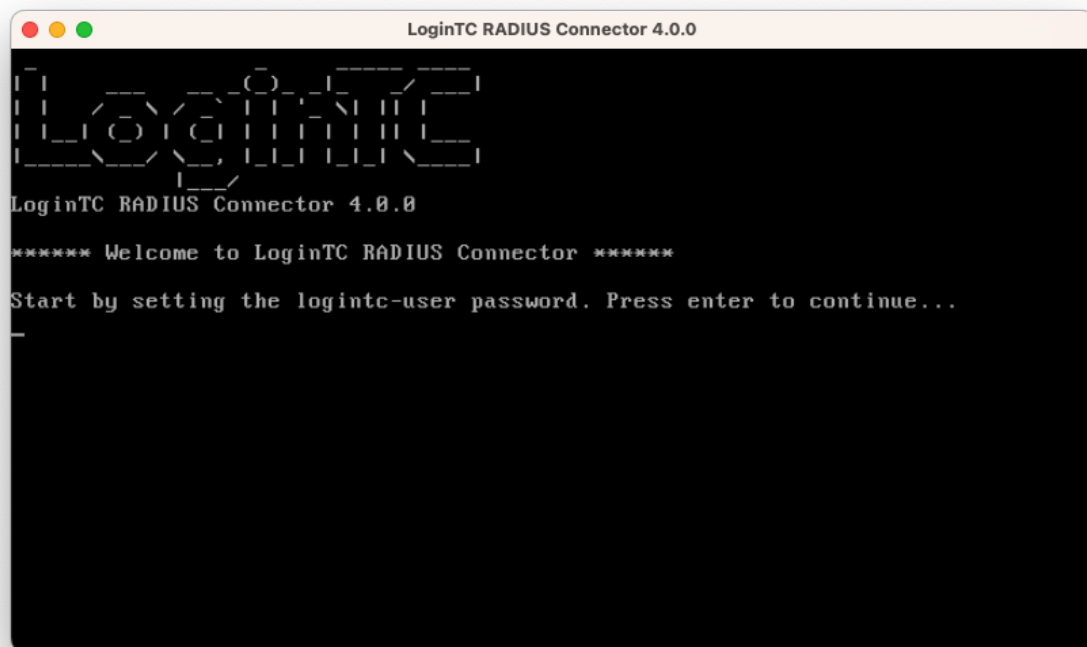
5. Login using the username **logintc-user** and default password **logintcradius**:



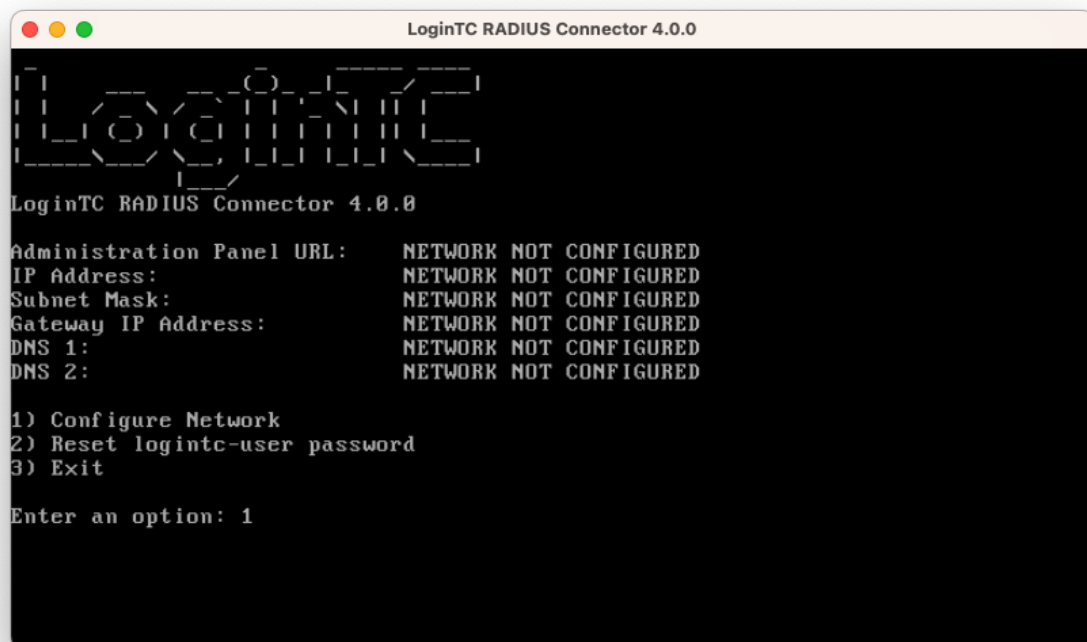
6. Once logged in type **setup**:



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



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



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 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

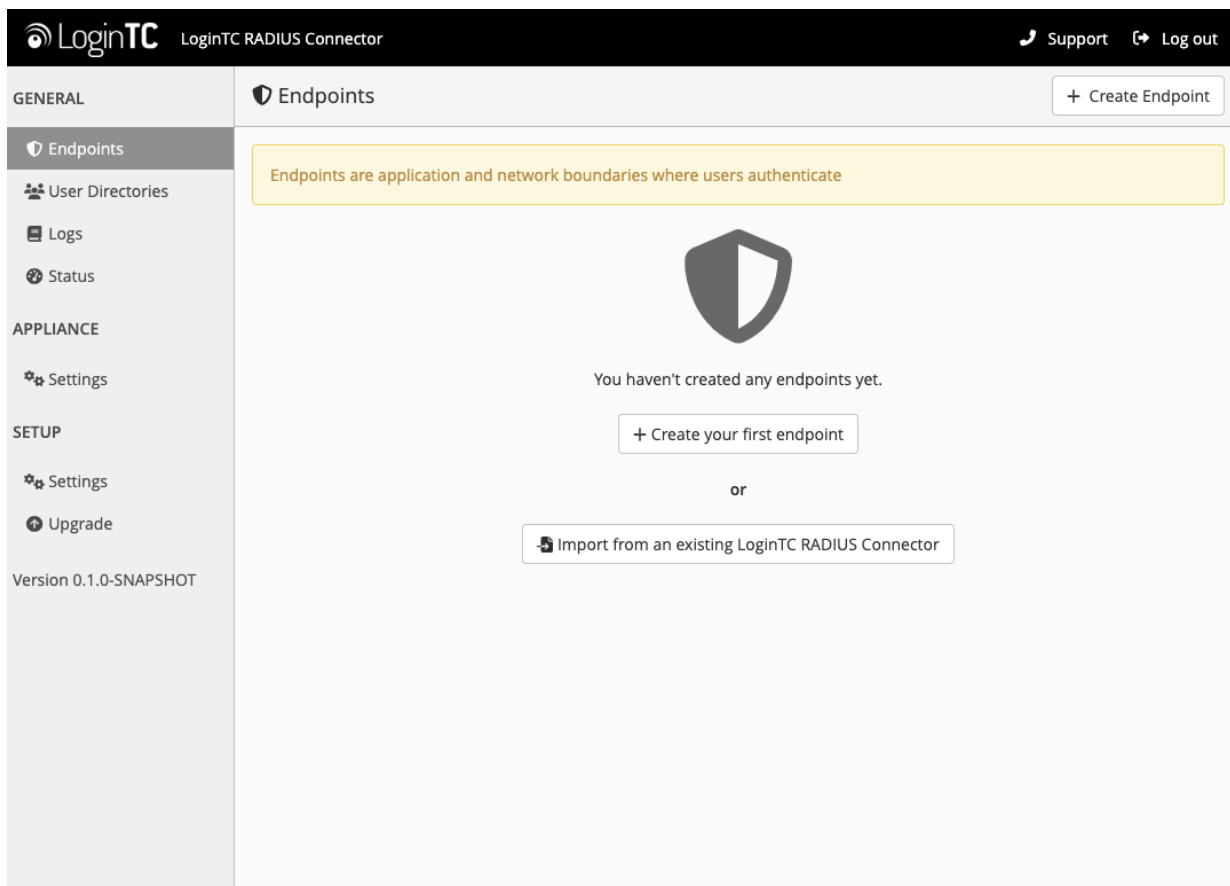
No, continue to the administration panel

[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 SSH 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 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



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:

Support

Log out

LoginTC

LoginTC RADIUS Connector

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:

15/42

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
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, retrieve Application ID
Application API Key	The 64-character Application API Key, retrieve Application API Key
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

16/42

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.

L

Generic LDAP
Leverage your LDAP server.

R

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**:

18/42

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

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", "Upgrade", and "Version 4.0.0"). The main content area is titled "Endpoints / Create / Challenge Strategy" and includes "Step 3 of 4", "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 presented: 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.

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)

Generic RADIUS

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 plus .	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)

Generic RADIUS

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

Press 1 to authenticate with the LoginTC app or enter an OTP or bypass code.

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**.

25/42

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints

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

Create Endpoint

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

Dashboard

Users

Applications

Policies

Groups

Bypass Codes

Devices

Phones

Hardware Tokens

User Logs

SETUP

Domains

Administrators

Admin Logs

Domains / Example Inc. Secure Access

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	john.doe	IOS-4f6aa853	Example Inc. Secure Access		4 seconds ago
CREATE_REQUEST	john.doe	IOS-4f6aa853	Example Inc. Secure Access		15 seconds ago

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' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). 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		+ Issue Token

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' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). 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	Revoke Token

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 blue header bar contains the status "No SIM", the time "2:28 PM", and icons for signal, Bluetooth, and battery. Below the header, a blue bar has three buttons: "Cancel", "Add Token", and "Next". The main content area has a title "Step 1 of 3: Enter Activation Code". Below the title, the alphanumeric 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 already have one. At the bottom, a virtual keyboard is shown with four rows of keys: QWERTYUIOP, ASDFGHJKL, an arrow key, ZXCVBNM, and a row with "123", a globe icon, a microphone icon, a "space" key, and a "Next" button.

No SIM 2:28 PM

Cancel Add Token Next

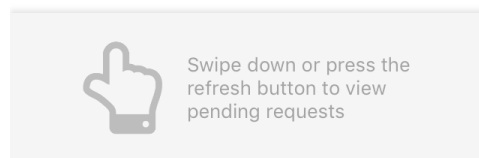
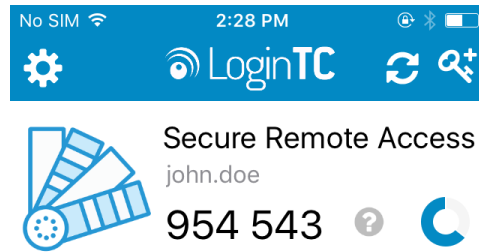
Step 1 of 3: Enter Activation Code

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

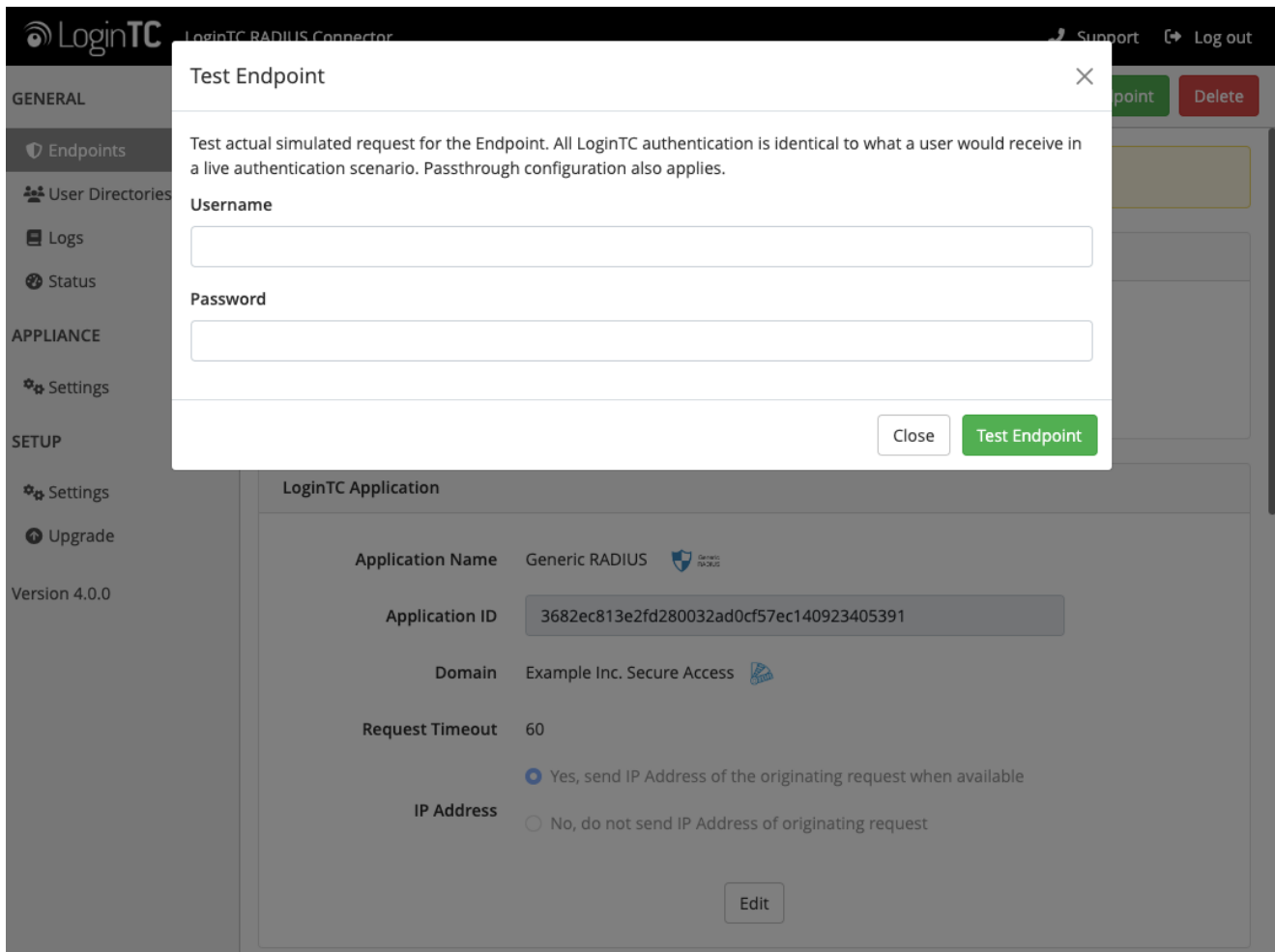
DomainExample Inc. Secure Access

Request Timeout60

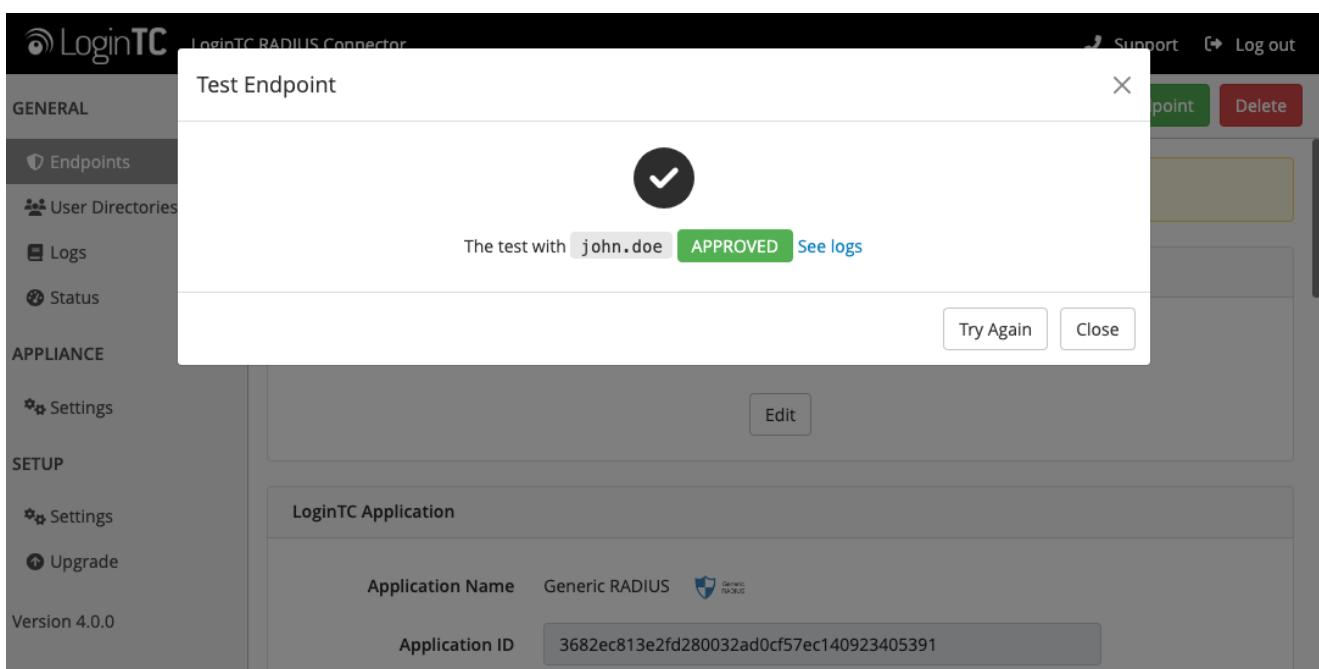
IP Address☒ Yes, send IP Address of the originating request when available
☐ No, do not send IP Address of originating request

Edit

Click **Test Configuration**:

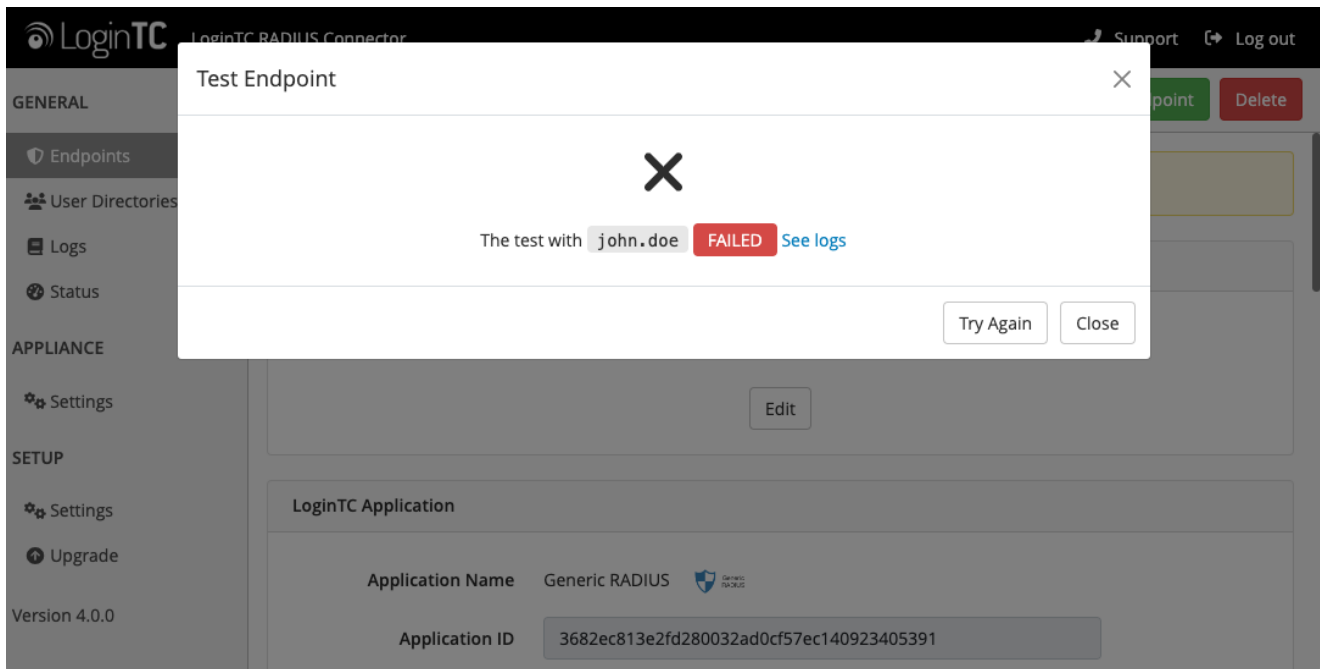


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

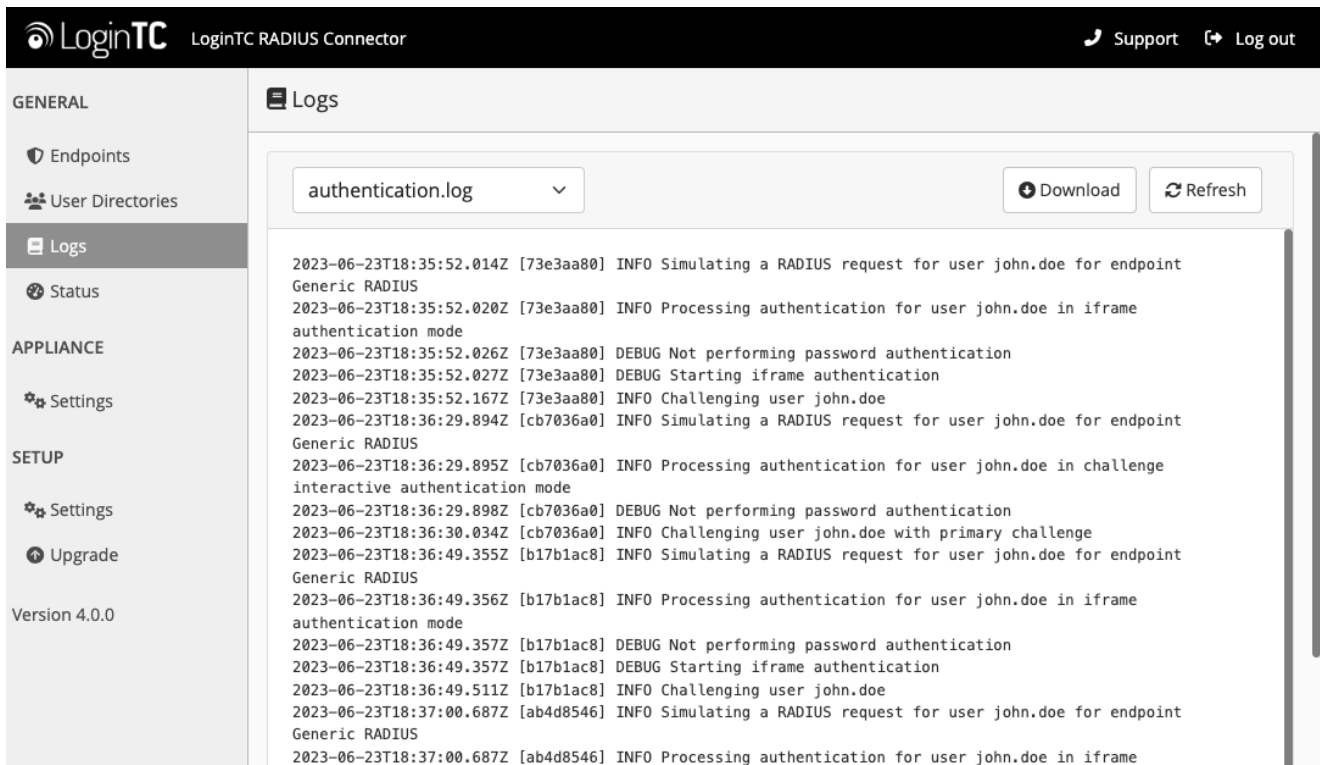


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



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



Install PAM RADIUS module

The PAM RADIUS module from FreeRADIUS allows the use of RADIUS to PAM authentication. It can be leverage for almost any service that supports PAM-based authentication. If your system does not have pam_radius_auth package installed you will need to do so. Below are instructions for CentOS. For more information on pam_radius_auth and installing it on your system please see: [FreeRADIUS PAM Authentication and Accounting module](#).

Advisory

PAM RADIUS is free software. LoginTC does not take responsibility for its support.

Using Ubuntu?

Check out this knowledge base article for configuring LoginTC with PAM RADIUS on Ubuntu: [Protect SSH to Ubuntu](#)

Install PAM RADIUS on CentOS / RedHat

Step 1: Developer tools:

```
$ sudo yum install wget gcc pam pam-devel make -y
```

Step 2: Build PAM RADIUS module pre:

```
$ cd /tmp
$ sudo wget ftp://ftp.freeradius.org/pub/radius/pam_radius-1.4.0.tar.gz
$ sudo tar xvzf pam_radius-1.4.0.tar.gz
$ cd pam_radius-1.4.0
$ sudo ./configure
$ sudo make
```

Note: PAM RADIUS module version 1.4.0

At the time of this document being written **1.4.0** was the latest version of the PAM RADIUS module. For updates please see: [FreeRADIUS PAM Authentication and Accounting module](#).

Step 3: Copy shared object library to appropriate folder

32-bit

```
$ sudo cp pam_radius_auth.so /lib/security/
```

64-bit

```
$ sudo cp pam_radius_auth.so /lib64/security/
```

The PAM RADIUS library is installed and ready to be configured.

Configure SSH

Step 1: Create or edit the `/etc/raddb/server` file to point to your LoginTC RADIUS Connector:

```
$ sudo mkdir -p /etc/raddb
$ sudo vi /etc/raddb/server

# server[:port] shared_secret      timeout (s)
# Example server (change to fit your needs):
192.168.1.40    bigsecret          60
```

The `server` should match the IP Address of your LoginTC RADIUS Connector, while the `shared_secret` should match to one configured in the LoginTC RADIUS Connector. The corresponding settings are configured in Client and Encryption portion of the LoginTC RADIUS Connector.

Note: Timeout

We recommend the maximum timeout of 60 seconds allowed by the PAM RADIUS module.

Step 2: Edit `/etc/pam.d/sshd` (NOTE: recommend making a backup of `/etc/pam.d/sshd` prior to editing`):`

```
$ sudo vi /etc/pam.d/sshd
```

Option 1: Use only LoginTC RADIUS Connector for authentication:

```
##PAM-1.0
#auth      substack      password-auth
auth       required      pam_radius_auth.so
auth       include       postlogin
account    required      pam_sepermit.so
account    required      pam_nologin.so
account    include       password-auth
password   include       password-auth
# pam_selinux.so close should be the first session rule
session    required      pam_selinux.so close
session    required      pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed
in the user context
session    required      pam_selinux.so open env_params
session    required      pam_namespace.so
session    optional      pam_keyinit.so force revoke
session    optional      pam_motd.so
session    include       password-auth
session    include       postlogin
```

Option 2: Use local password authentication AND LoginTC RADIUS Connector for authentication:

```
##PAM-1.0
auth      substack      password-auth
auth      required      pam_radius_auth.so
auth      include       postlogin
account   required      pam_sepermit.so
account   required      pam_nologin.so
account   include       password-auth
password  include       password-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed
in the user context
session   required      pam_selinux.so open env_params
session   required      pam_namespace.so
session   optional      pam_keyinit.so force revoke
session   optional      pam_motd.so
session   include       password-auth
session   include       postlogin
```

Challenge Mode

Client Settings **Authentication Mode** should be set to **Challenge**.

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints / Create / Client Settings

Step 4 of 4
Back
Cancel

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade

Version 4.0.0

Generic RADIUS Details

Name (optional)

Generic RADIUS

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

Press 1 to authenticate with the LoginTC app or enter an OTP or bypass code.

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.

Challenge Message: Press 1 to authenticate with LoginTC Push or enter an OTP or bypass code:

Also ensure `/etc/ssh/sshd_config` has `ChallengeResponseAuthentication yes` set.

Step 3: Restart `sshd`:

```
$ sudo service sshd restart
```

You are now ready to test two-factor authentication with SSH.

Testing

There are many flavours of Linux, RHEL, CentOS and we recommend extensive testing prior to applying these configurations in a production environment. Console login should be accessible during testing as a fallback.

Testing SSH

Test by accessing SSH. The username of the UNIX user must match the username of the user created in your organization and added to the domain you have configured to authenticate against.

```
$ ssh john.doe@192.168.0.30
```

You will be prompted for a password and then challenged with LoginTC.

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](#).

Uninstallation

Step 1: Revert the changes made to `/etc/pam.d/sshd` in Step 2 of [Configure SSH](#)

```
$ sudo vi /etc/pam.d/sshd
```

Step 2: Restart `sshd`:

```
$ sudo service sshd restart
```

Logging

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

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". On the left sidebar, the "Logs" tab is selected, with other options like "GENERAL", "Endpoints", "User Directories", "Status", "APPLIANCE", "Settings", "SETUP", and "Upgrade". The main content area shows a list of logs for the file "authentication.log". Each log entry includes a timestamp, a log level in brackets, and a message. The messages describe simulated RADIUS requests and authentication processes for a user named "john.doe" across different endpoints and modes (Generic RADIUS, iframe authentication, challenge interactive authentication). The interface also features a "Download" button and a "Refresh" button.

Timestamp	Log Level	Message
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

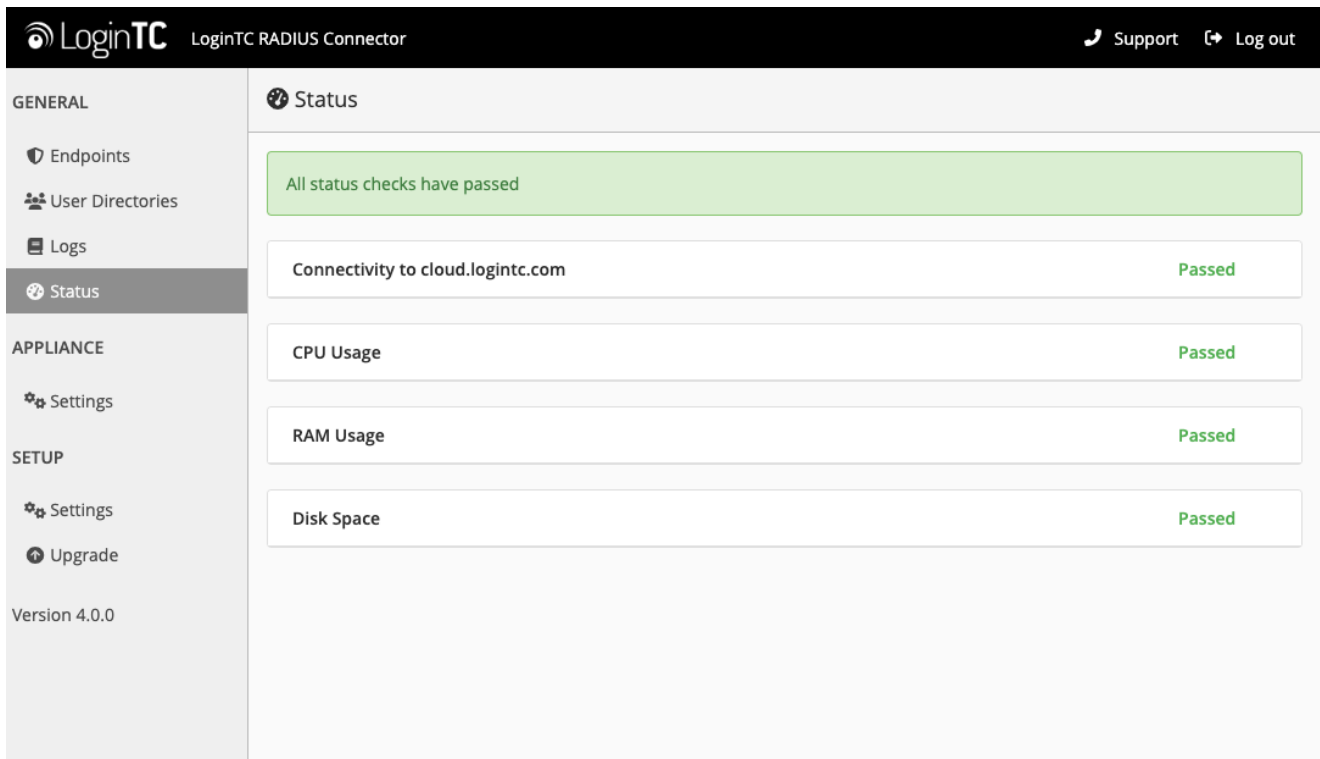
Troubleshooting

PAM RADIUS Module

For troubleshooting related to the PAM RADIUS module please refer to: [FreeRADIUS PAM Authentication and Accounting module](#).

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 the following items: "GENERAL" (with a sub-menu: "Endpoints", "User Directories", "Logs", and "Status"), "APPLIANCE" (with a sub-menu: "Settings"), and "SETUP" (with sub-menus: "Settings" and "Upgrade"). The "Status" option is currently selected. The main content area, titled "Status", shows a green banner stating "All status checks have passed". Below this, there are three status checks, each in a white box with a green "Passed" label on the right: "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**:

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints
User Directories
Logs
Status

APPLIANCE

Settings

SETUP

Settings
Upgrade

Version 4.0.0

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

```

Also make sure to check the secure logs on the Linux machine hosting SSH (`/var/log/secure`).

Email Support

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

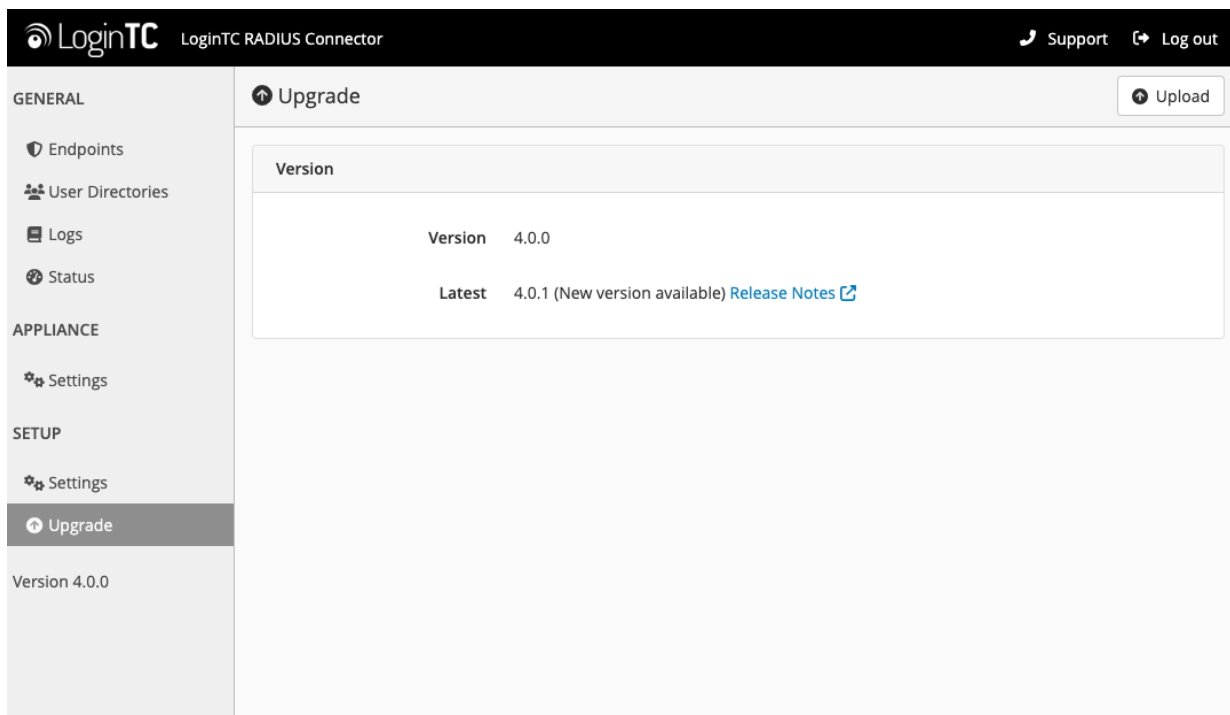
Upgrading

From 4.X

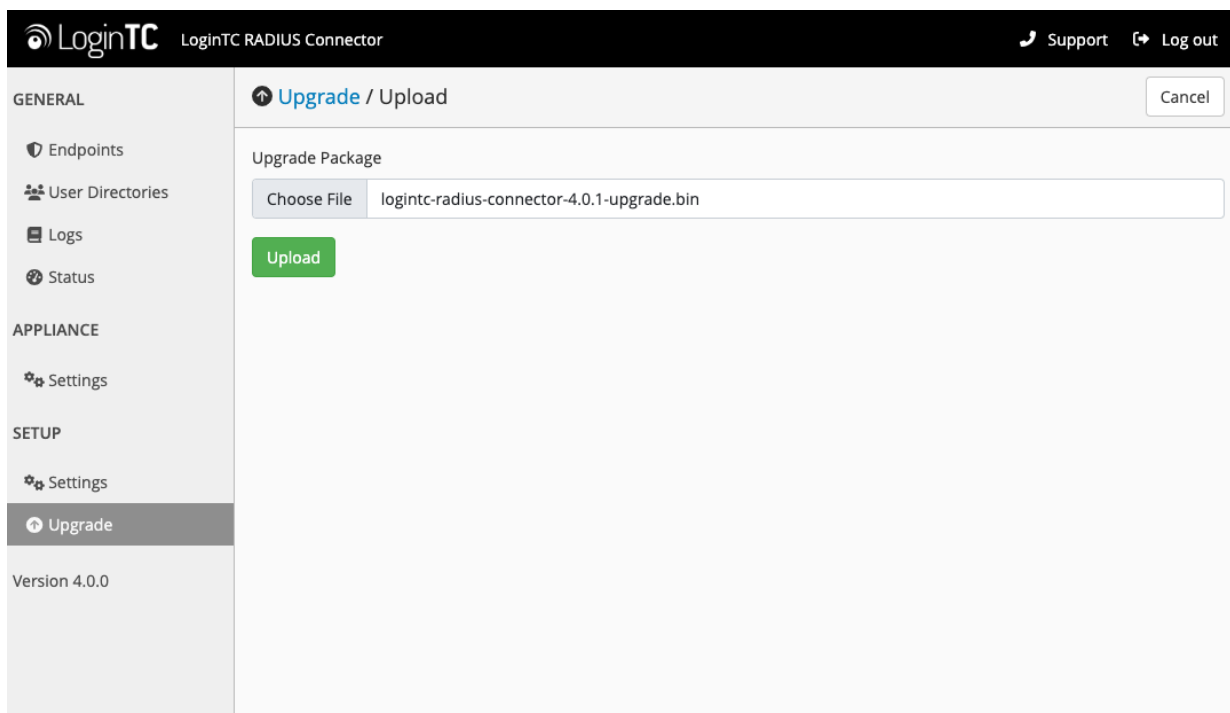
The latest LoginTC RADIUS Connector upgrade package can be downloaded here: [Download RADIUS Connector \(Upgrade\)](#).

39/42

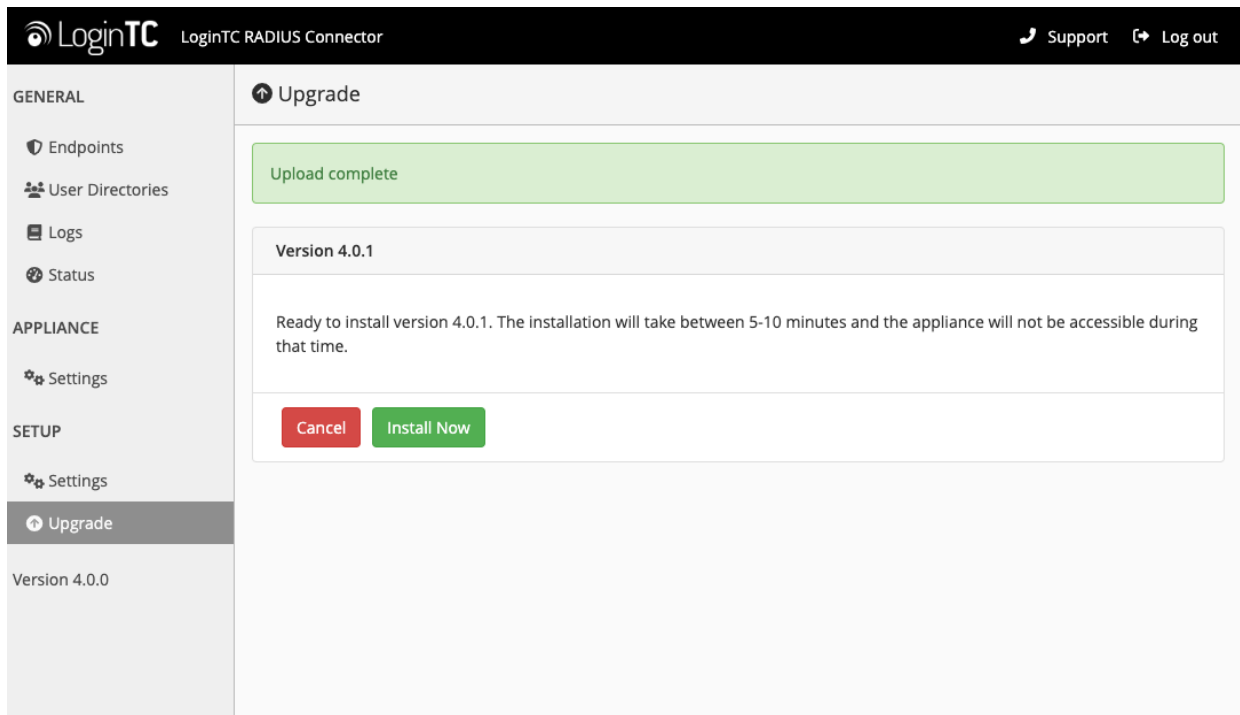
1. Navigate to **SETUP > Upgrade**:



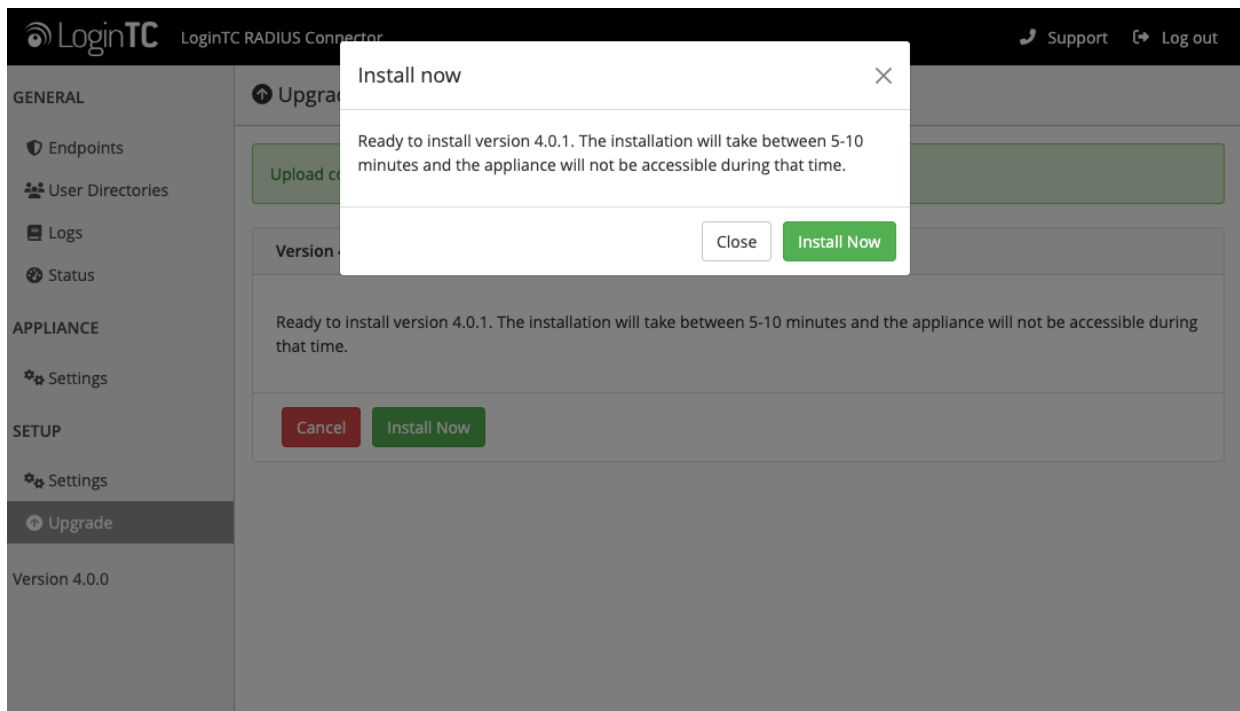
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



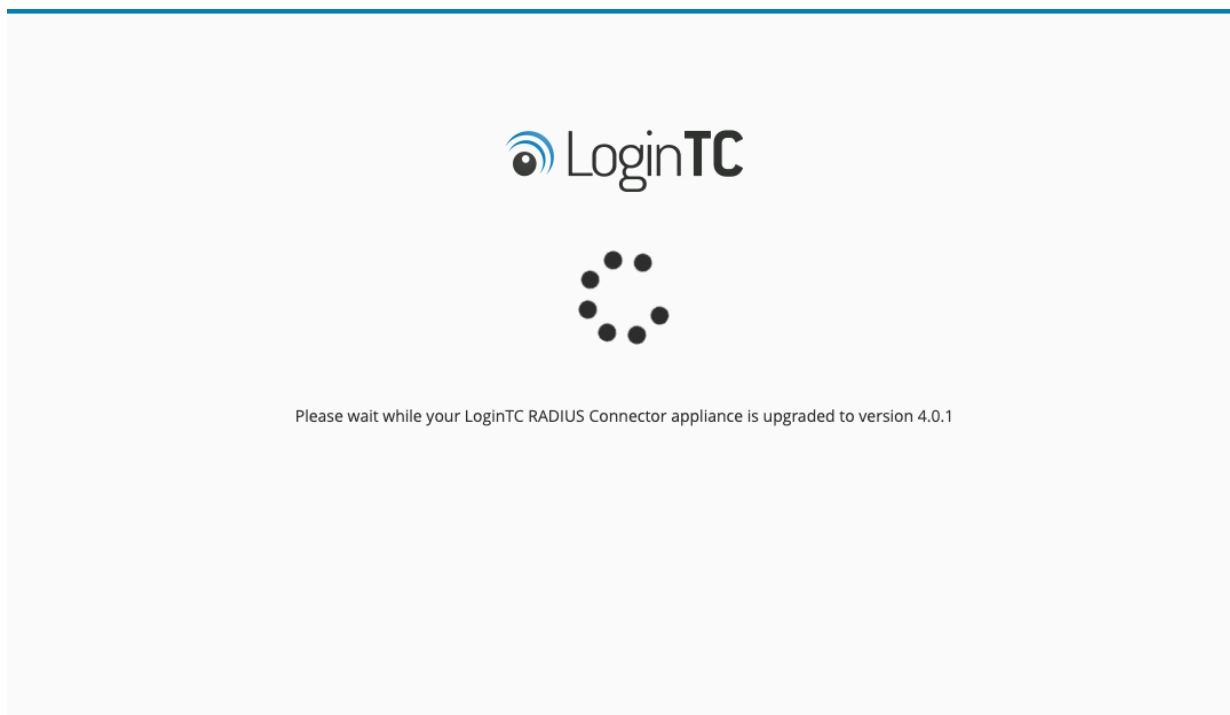
3. Click **Upload** and do not navigate away from the page:



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](#)