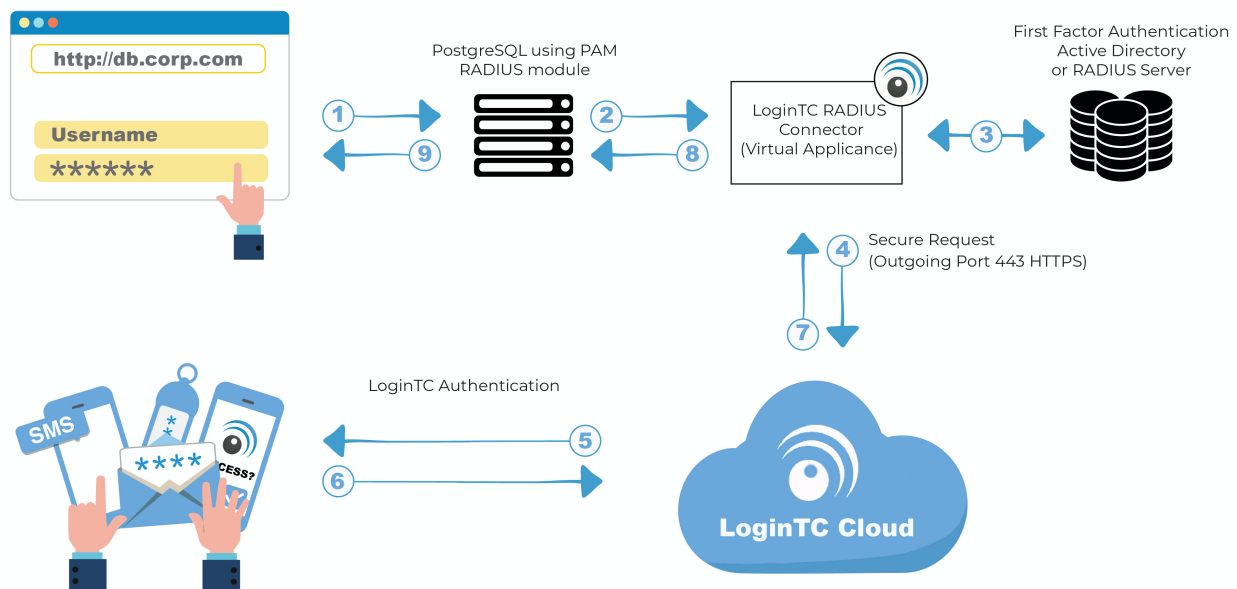


PostgreSQL Two-Factor Authentication (2FA) - LoginTC

logintc.com/docs/connectors/postgresql

LoginTC makes it easy for administrators to add multi-factor to PostgreSQL on their Unix systems. This document shows how to configure PostgreSQL to require two factor authentication for local and / or remote access via Pluggable Authentication Module (PAM). MySQL can be configured in a similar fashion.

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 to PostgreSQL

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

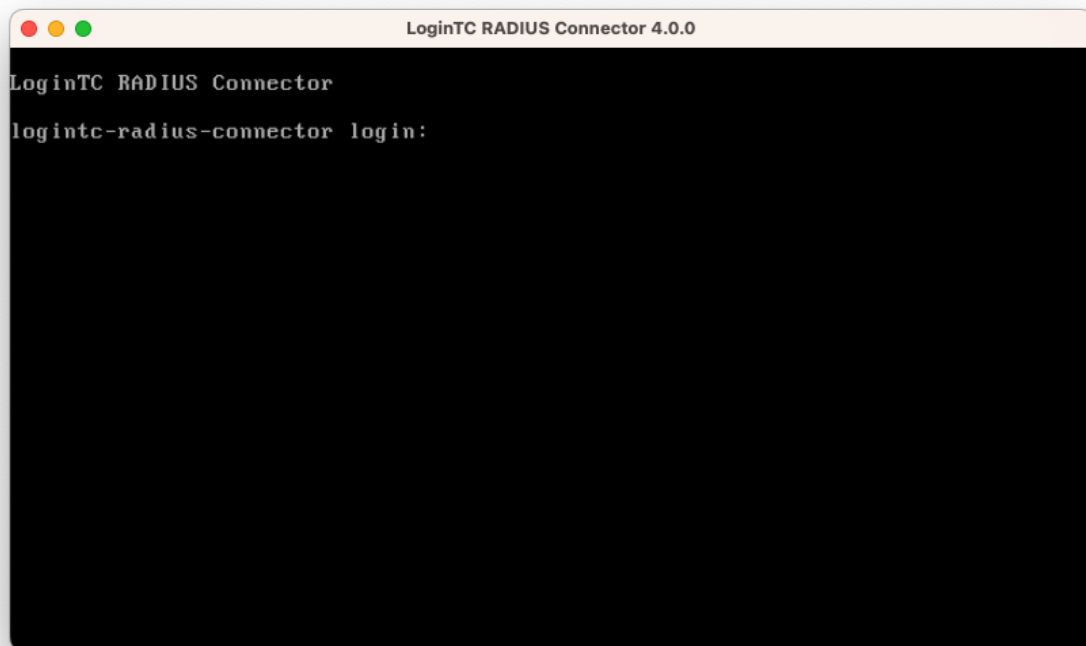
Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

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](#).

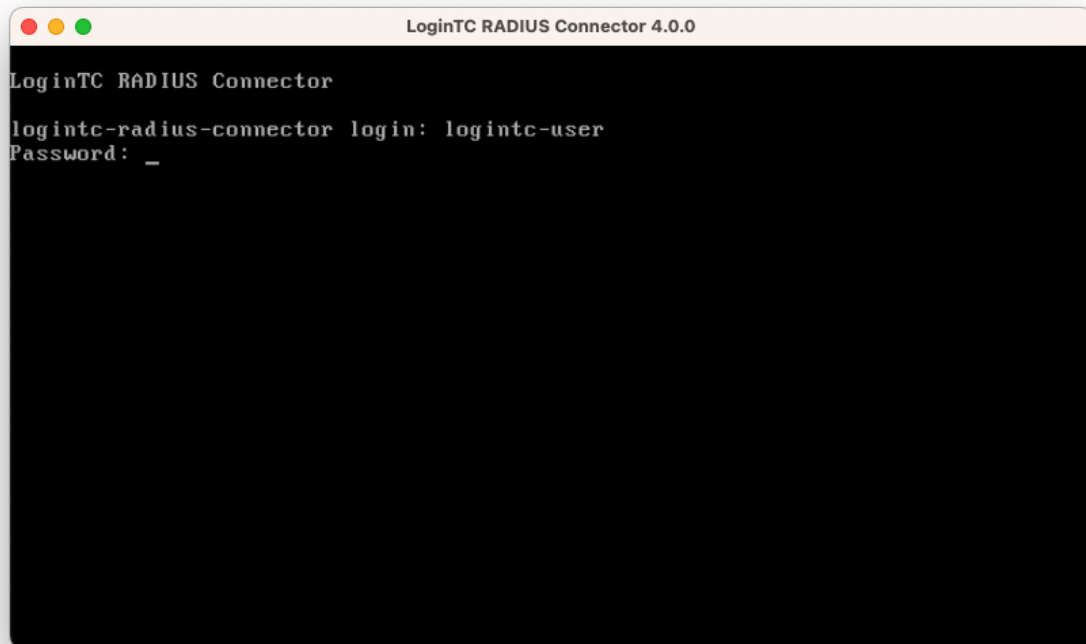
Installation

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:



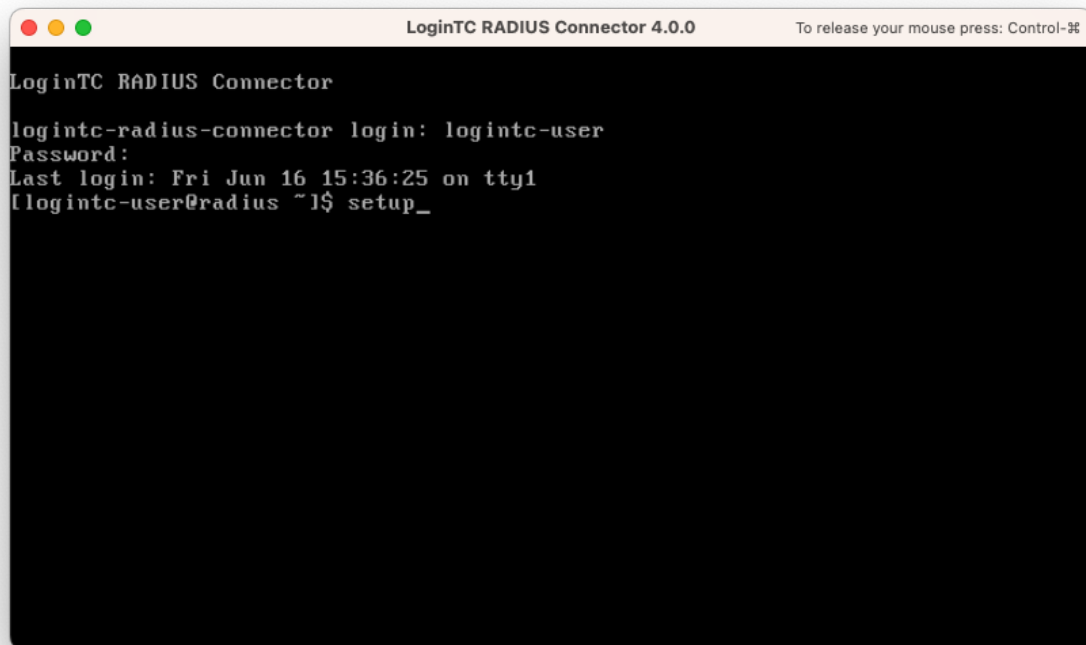
```
LoginTC RADIUS Connector 4.0.0
LoginTC RADIUS Connector
logintc-radius-connector login:
```

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

A terminal window titled "LoginTC RADIUS Connector 4.0.0" with a black background and white text. The text shows the login process: "LoginTC RADIUS Connector", "logintc-radius-connector login: logintc-user", and "Password: _".

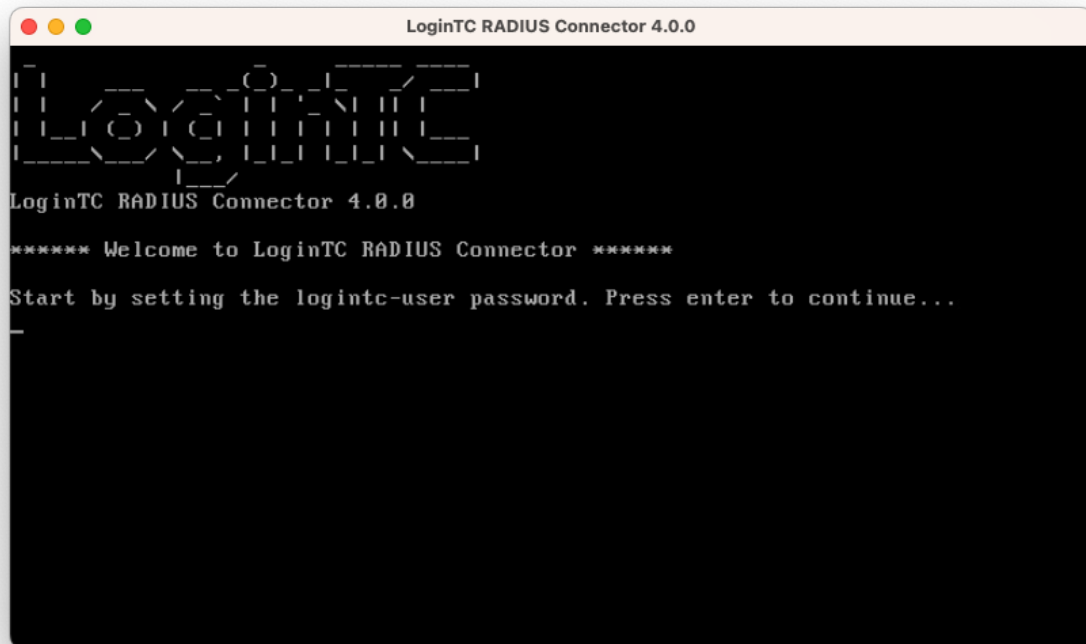
```
LoginTC RADIUS Connector
logintc-radius-connector login: logintc-user
Password: _
```

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

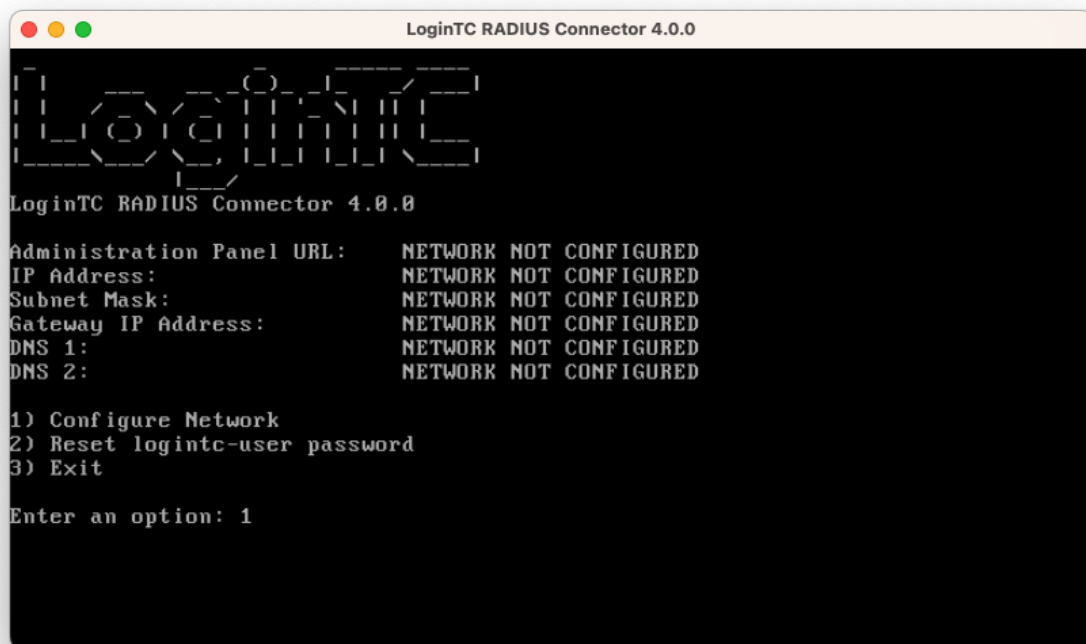
A terminal window titled "LoginTC RADIUS Connector 4.0.0" with a black background and white text. The text shows the login process followed by the setup command: "LoginTC RADIUS Connector", "logintc-radius-connector login: logintc-user", "Password:", "Last login: Fri Jun 16 15:36:25 on tty1", and "[logintc-user@radius ~] \$ setup_".

```
LoginTC RADIUS Connector
logintc-radius-connector login: logintc-user
Password:
Last login: Fri Jun 16 15:36:25 on tty1
[logintc-user@radius ~] $ setup_
```

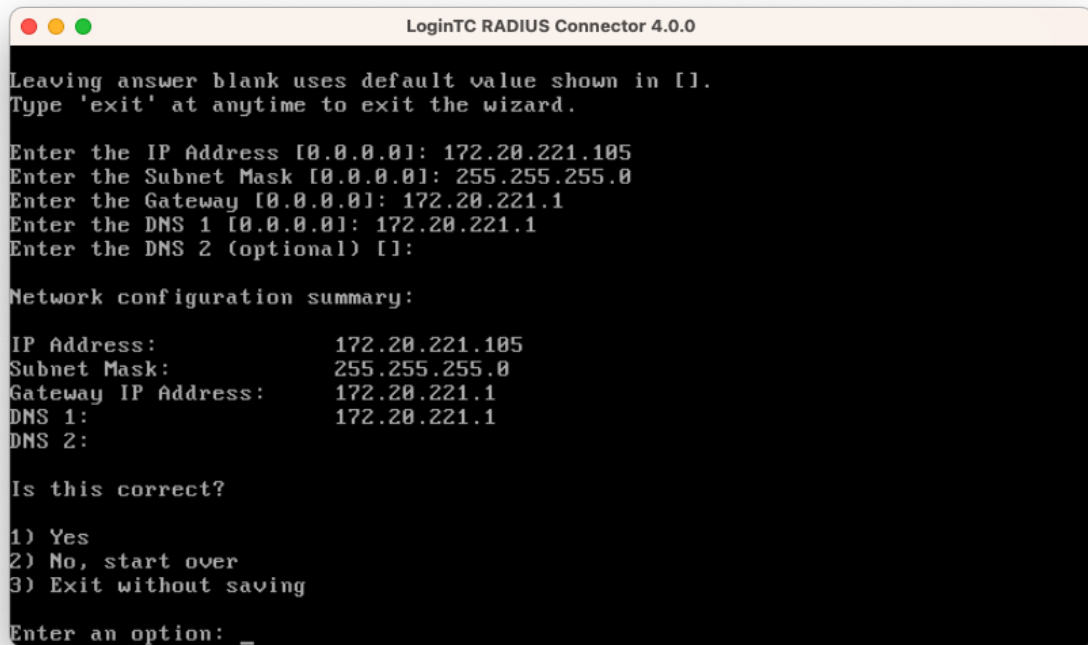
7. Follow the on-screen prompt to setup a new password for **logintc-user**:



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:

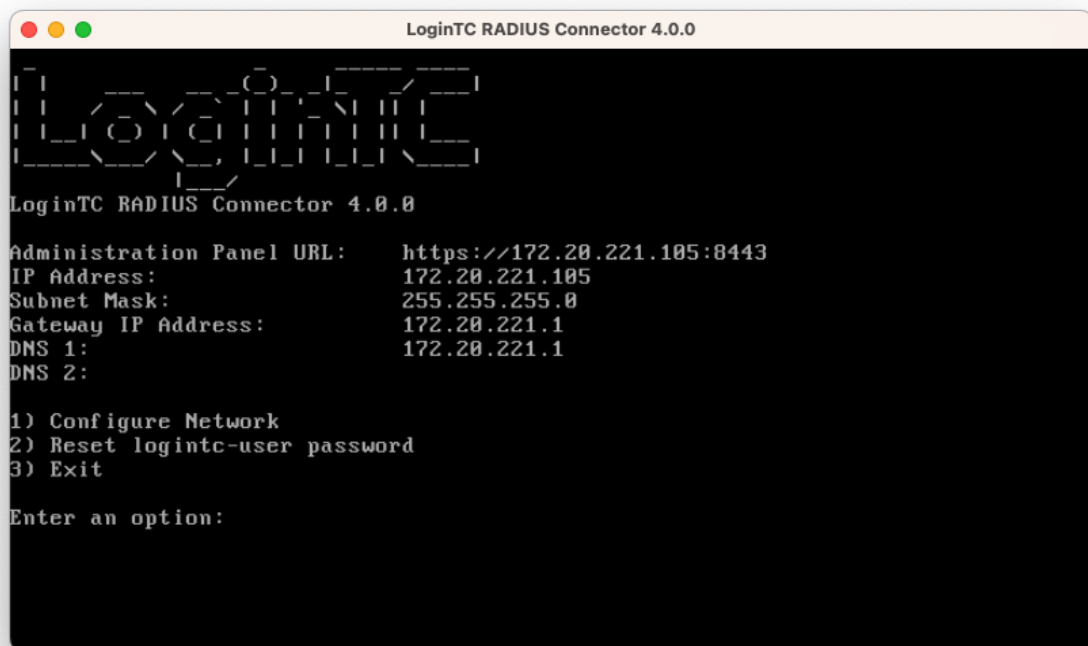
IP Address:          172.20.221.105
Subnet Mask:         255.255.255.0
Gateway IP Address:  172.20.221.1
DNS 1:               172.20.221.1
DNS 2:

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

Password

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 your wish to import configurations then click **Yes, import configurations from an existing LoginTC RADIUS Connector**, otherwise click **No, continue to the adminisitation 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

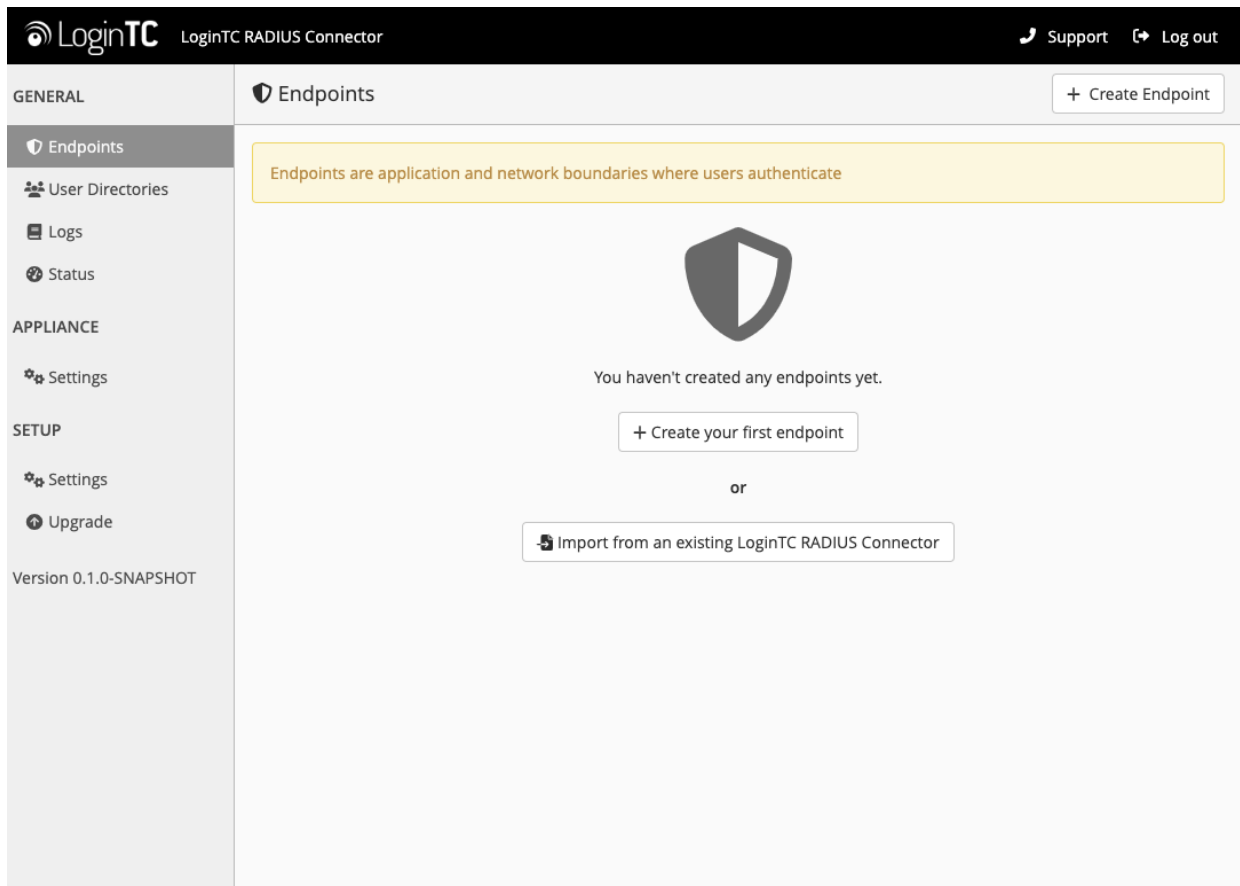
No, continue to the administration panel

[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 PostgreSQL PAM Authentication

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:**

GENERAL 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](#)






Version 4.0.0

LoginTC Settings

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

GENERAL 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:

LoginTC LoginTC RADIUS Connector Support Log out

GENERAL Endpoints / Create / LoginTC Application Step 1 of 4 Back Cancel



Generic RADIUS
Generic RADIUS Example Inc. Secure Access

Endpoints

- User Directories
- Logs
- Status

APPLIANCE

- Settings

SETUP

- Settings
- Upgrade

Version 4.0.0

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:

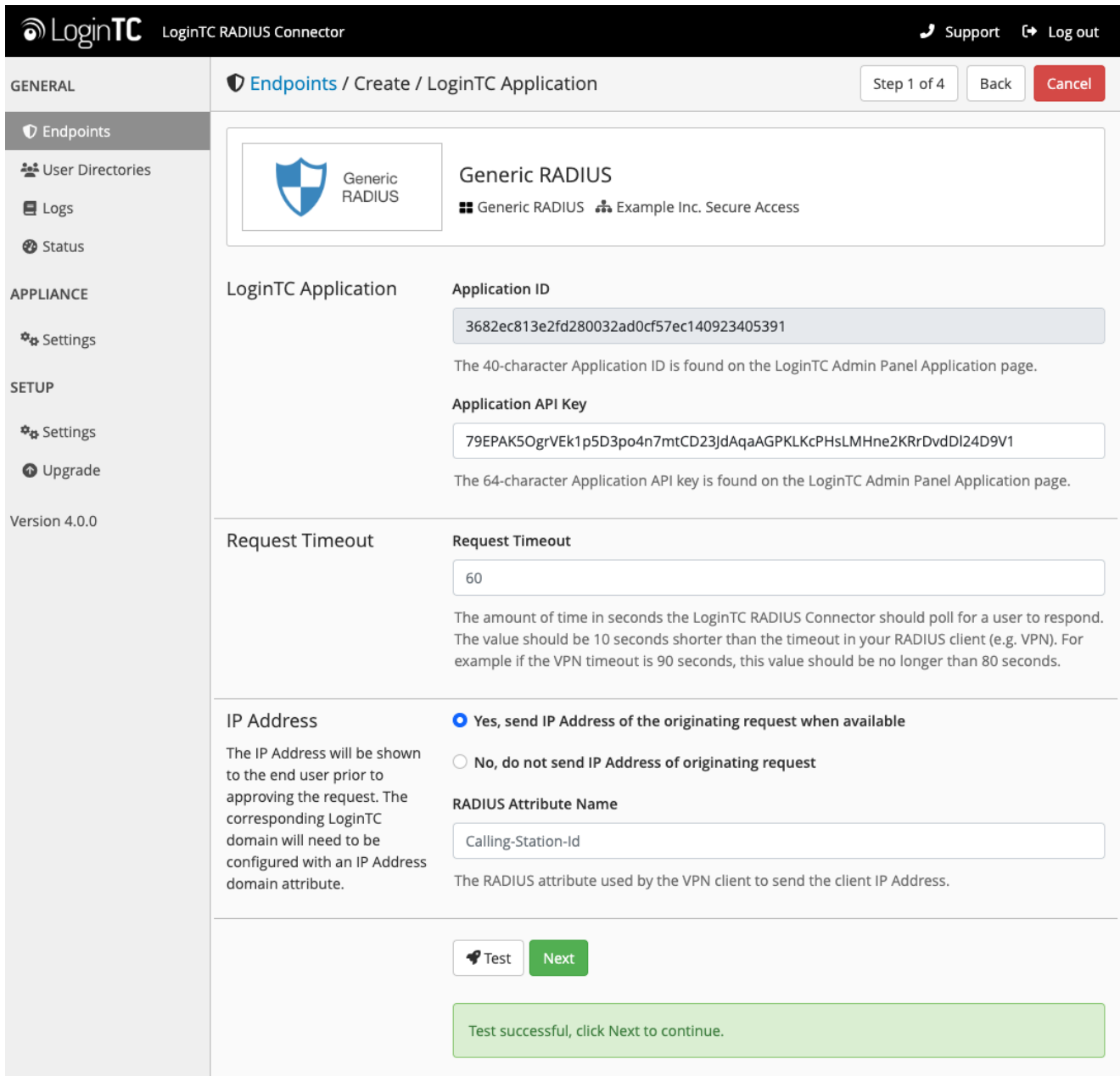
Property	Explanation
Application ID	The 40-character Application ID, retrieve Application ID
Application API Key	The 64-character Application API Key, retrieve Application API Key
Request Timeout	Number of seconds that the RADIUS connector will wait for

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

Request Timeout

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 / 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

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 LoginTC RADIUS Connector Support Log out

GENERAL Endpoints / Create / User Directory Step 2 of 4 Back Cancel

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings


SETUP


Settings


Upgrade

Version 4.0.0


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**:

LoginTC LoginTC RADIUS Connector Support Log out

User Directories / Create / Configure Active Directory Server Step 2 of 2 Back Cancel

GENERAL

- Endpoints
- User Directories**
- Logs
- Status

APPLIANCE

- Settings

SETUP

- Settings
- Upgrade

Version 4.0.0

Connection Details

Name (optional)

 Name of the Active Directory server.

IP Address or Host Name

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

Port (optional)

 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:

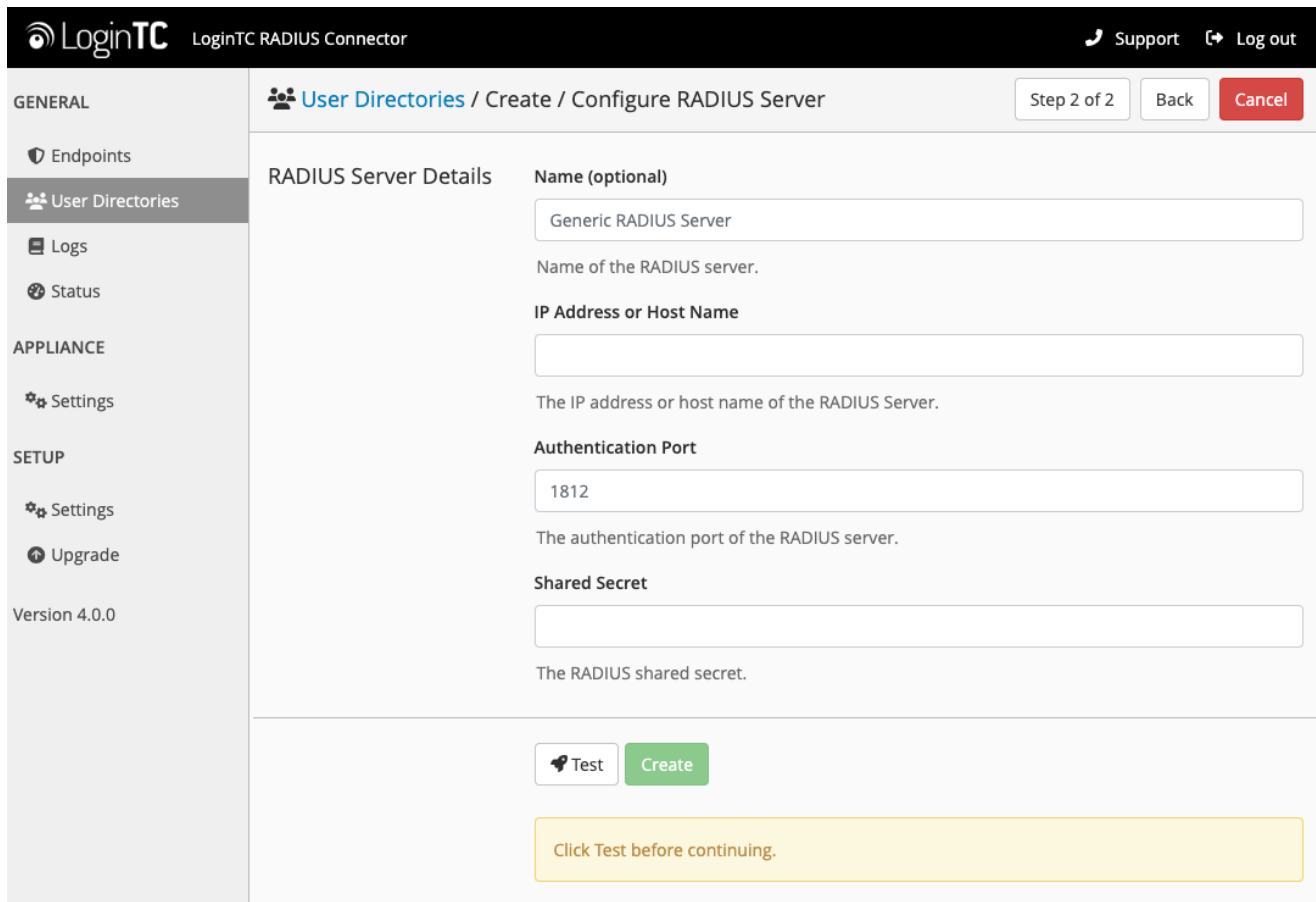
Property	Explanation	Examples
host	Host or IP address of the LDAP server	ldap.example.com or 192.168.1.42
port (optional)	Port if LDAP server uses non-standard (i.e., 389/636)	4000
bind_dn	DN of a user with read access to the directory	cn=admin,dc=example,dc=com
bind_password	The password for the above 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>
<code>LDAP Group</code> (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 LoginTC RADIUS Connector Support Log out

GENERAL Step 2 of 2 Back Cancel

User Directories / Create / Configure RADIUS Server

RADIUS Server Details

Name (optional)

 Name of the RADIUS server.

IP Address or Host Name

 The IP address or host name of the RADIUS Server.

Authentication Port

 The authentication port of the RADIUS server.

Shared Secret

 The RADIUS shared secret.

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 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 'GENERAL' (selected), 'Endpoints', 'User Directories', 'Logs', and 'Status'. Below this are sections for 'APPLIANCE' (Settings) and 'SETUP' (Settings, Upgrade). The main content area is titled 'Endpoints / Create / Challenge Strategy' and shows three options for challenge strategies: 'Challenge All Users' (selected), 'Challenge Users Based on Static Username List', and 'Challenge Users Based on Group Membership'. A yellow instruction box at the top reads: 'Select which users should be challenges with LoginTC and which should bypass LoginTC'. The interface also features 'Step 3 of 4', 'Back', and 'Cancel' buttons.

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 interface. The top navigation bar includes the LoginTC logo, 'LoginTC RADIUS Connector', 'Support', and 'Log out'. The main content area is titled 'Endpoints / Create / Challenge Strategy' and is on 'Step 3 of 4'. The left sidebar contains navigation items: 'Endpoints', 'User Directories', 'Logs', 'Status', 'APPLIANCE', 'Settings', 'SETUP', 'Settings', and 'Upgrade'. The main content area is divided into two sections: 'Static Username List' and 'Challenge Users'. The 'Static Username List' section contains the text: 'Only users in a static username list will be challenged with LoginTC.' The 'Challenge Users' section contains a text area with the following example usernames: jane.doe, jane.smith, john.doe, john.smith. Below the text area are 'Test' and 'Next' buttons. A yellow warning box at the bottom of the main content area says '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

Step 4 of 4
Back
Cancel

Endpoints / Create / Client Settings

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

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

How the LoginTC authentication is performed

Direct
 Iframe
 Challenge
 Challenge Interactive

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 **Direct**

GENERAL | Endpoints / Create / Client Settings | Step 4 of 4 | Back | Cancel

Endpoints

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.

Version 4.0.0

The LoginTC RADIUS Connector will directly and automatically perform the LoginTC second factor. See [User Experience](#) for more information.

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

GENERAL | Endpoints | + Create Endpoint

Endpoints are application and network boundaries where users authenticate

Successfully created endpoint.

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

Version 4.0.0

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**

The screenshot shows the LoginTC Admin Panel interface. The top navigation bar includes the LoginTC logo, 'Example Inc. Business', and links for 'Docs', 'Support', and the user 'administrator@example.com'. The left sidebar is divided into 'GENERAL' and 'SETUP' sections. The 'Domains / Example Inc. Secure Access' page is active, showing a '+ Create Member' button and a 'Members' section with the text 'Example Inc. Secure Access has 88 member(s)' and a '+ Create Member' / 'View Members' button. Below this is an 'Attributes' section stating 'Example Inc. Secure Access doesn't have any domain attributes yet.' with a '+ Create Domain Attribute' button. The 'Latest Actions' section contains a table:

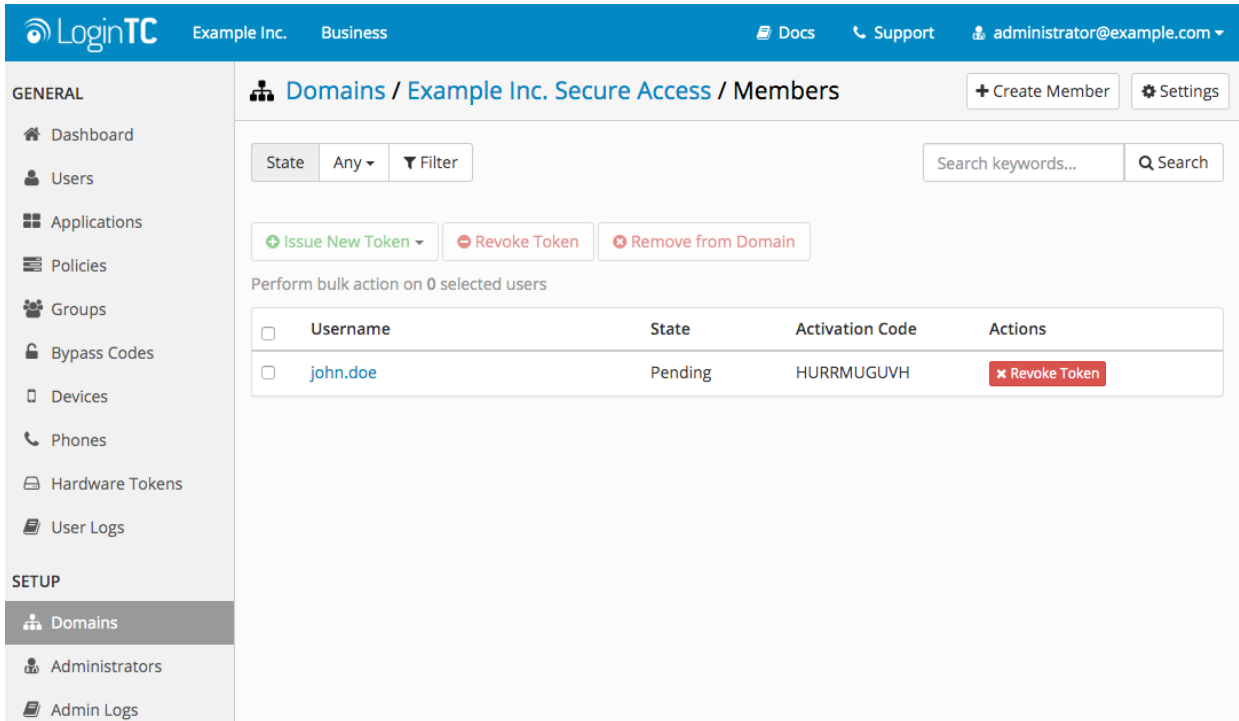
Action	User	Device/Phone	Domain	Group	Date
APPROVE_REQUEST_TEST	john.doe	IOS-4f6aa853	Example Inc. Secure Access		4 seconds ago
CREATE_REQUEST	john.doe	IOS-4f6aa853	Example Inc. Secure Access		15 seconds ago

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

The screenshot shows the LoginTC Admin Panel interface, specifically the 'Members' page for a domain. The top navigation bar is the same as in the previous screenshot. The left sidebar is also the same. The 'Domains / Example Inc. Secure Access / Members' page is active, showing a '+ Create Member' button and a 'Settings' button. Below this are filters for 'State' (Any) and 'Filter', and a search bar. There are three buttons: '+ Issue New Token', '- Revoke Token', and '+ Remove from Domain'. Below these is a message 'Perform bulk action on 0 selected users'. A table lists the members:

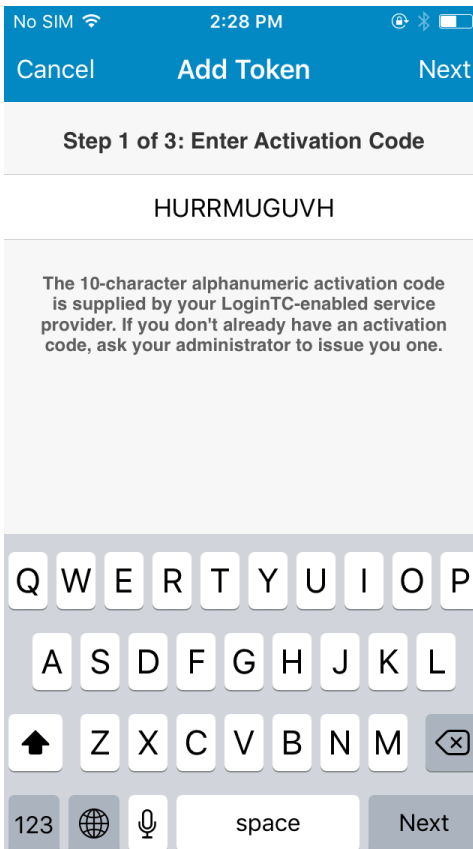
<input type="checkbox"/>	Username	State	Activation Code	Actions
<input type="checkbox"/>	john.doe	Inactive		+ Issue Token

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

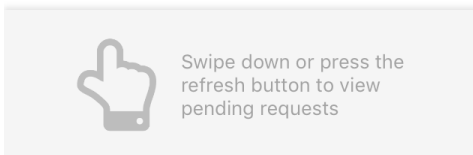
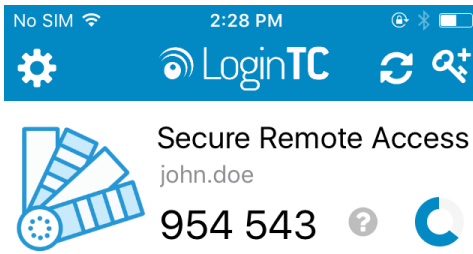


7. Open the LoginTC mobile app.

8. Enter the 10-character alphanumeric activation code:



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:

GENERAL

Endpoints / Generic RADIUS

Test Endpoint

Delete

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 Name Generic RADIUS

Edit

LoginTC Application

Application Name Generic RADIUS 

Application ID 3682ec813e2fd280032ad0cf57ec140923405391

Domain Example Inc. Secure Access 

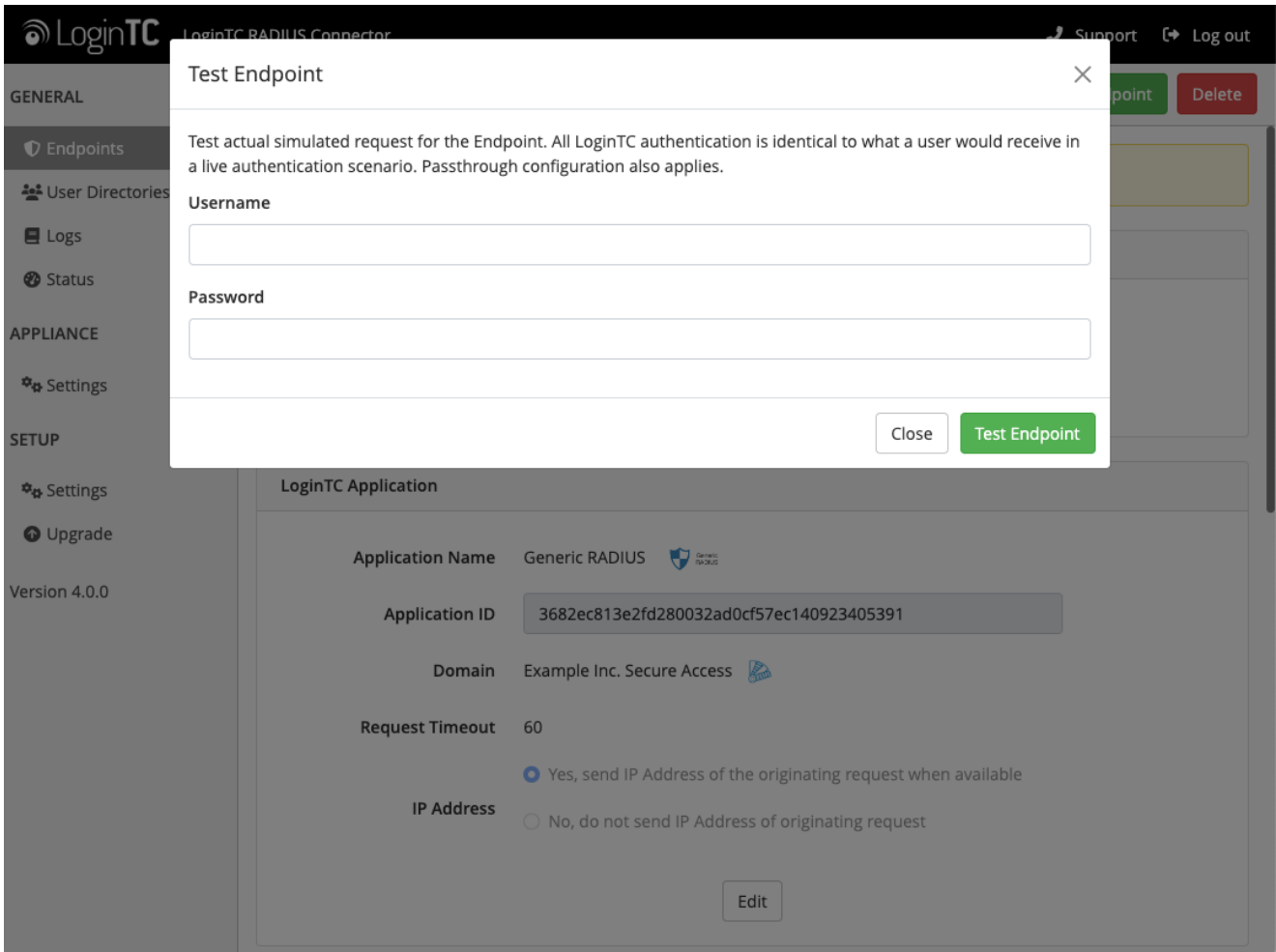
Request Timeout 60

Yes, send IP Address of the originating request when available

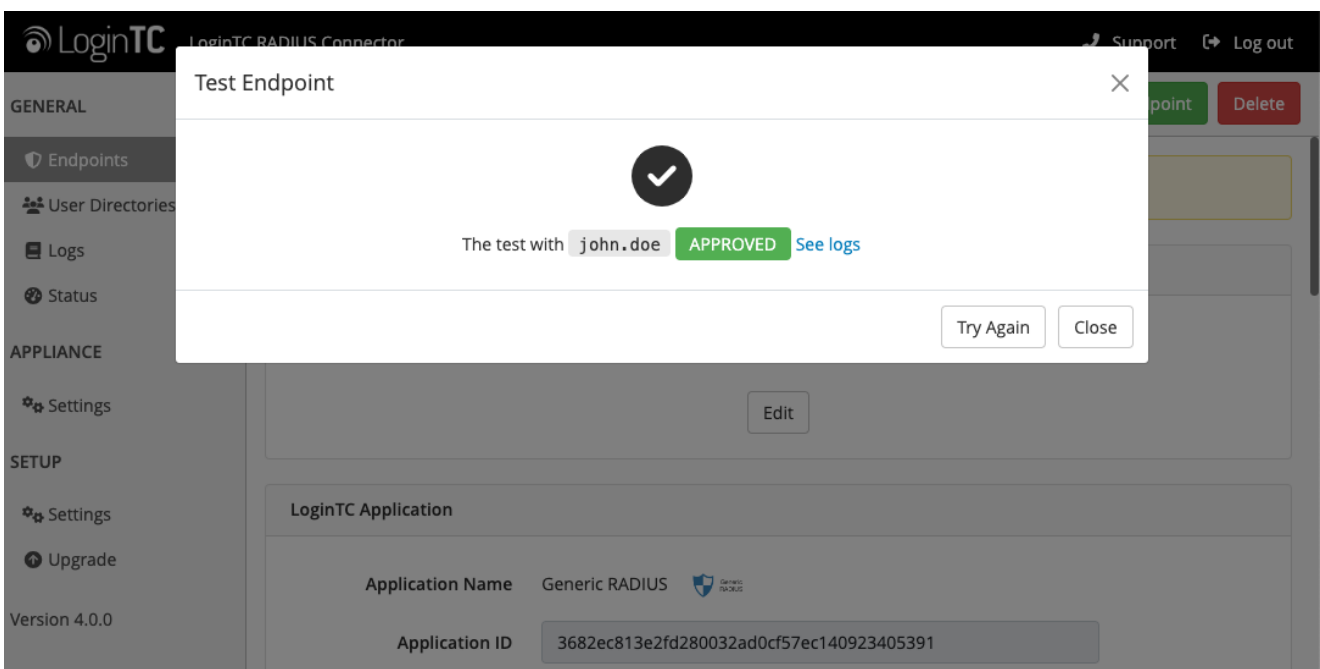
IP Address No, do not send IP Address of originating request

Edit

Click **Test Configuration**:

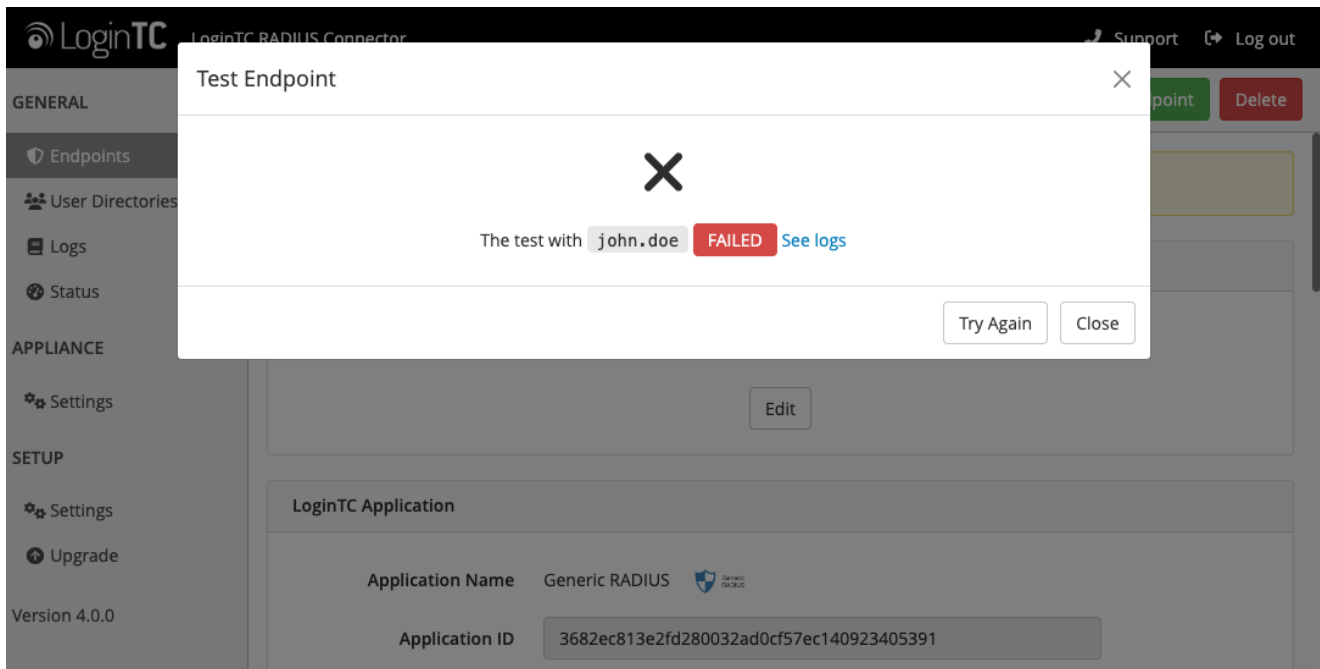


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

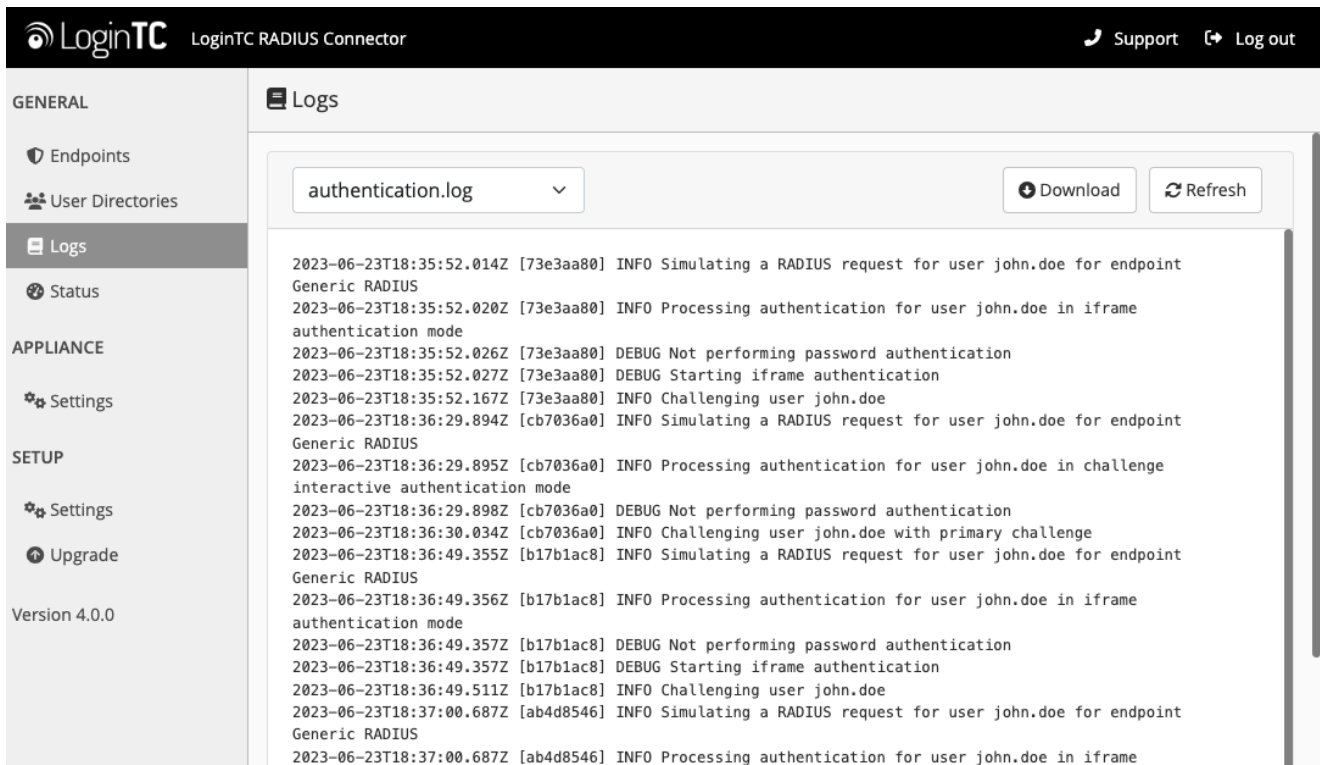


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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 RedHat. For more information on pam_radius_auth and installing it on your system please see: [FreeRADIUS PAM Authentication and Accounting module](#).

Install PAM RADIUS on 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.

PostgreSQL PAM Authentication Configuration

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/postgresql`:

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

Option 1: Use only LoginTC RADIUS Connector for authentication:

```
##PAM-1.0
auth      required      pam_radius_auth.so
account   include        system-auth
password  include        system-auth
session   include        system-auth
```

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

```
##PAM-1.0
auth      required      pam_radius_auth.so
auth      include        password-auth
account   include        system-auth
password  include        system-auth
session   include        system-auth
```

Note: Allow **postgres** process read-access to `/etc/shadow`

In order to leverage PAM authentication additional configuration may be required. The PAM RADIUS module uses `unix_chkpwd` to handle authentication, which in turn requires read access to `/etc/shadow`. Since the process running the PAM RADIUS module will be `postgres` it will require read-access to `/etc/shadow`. Opening up read-access to `/etc/shadow` does impose a security risk.

```
$ sudo groupadd -r shadow
$ sudo usermod -a -G shadow postgres
$ sudo chown root:shadow /etc/shadow
$ sudo chmod g+r /etc/shadow
```


Step 3: Configure PostgreSQL to use PAM RADIUS authentication module, edit `pg_hba.conf`:

```
$ sudo vi /var/lib/pgsql/data/pg_hba.conf
```

Add the following line where you would like to enforce two-factor authentication for PostgreSQL:

```
local all all [CIDR-ADDRESS] pam pamservice=postgresql
```

Example which requires two-factor authentication for local access and remote access from any IP Address within `192.168.x.x`:

```
# TYPE DATABASE USER CIDR-ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all pam
pamservice=postgresql
# IPv4 connections:
host all all 192.168.0.0/24 pam
pamservice=postgresql
```

Step 4: Restart `postgresql`:

```
$ sudo service postgresql restart
```

You are now ready to test two-factor authentication to PostgreSQL.

Testing PostgreSQL

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

```
$ psql -d testdb -U john.doe
```

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](#).

Logging

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

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 'GENERAL' section with 'Endpoints', 'User Directories', 'Logs' (selected), and 'Status'. Below this is an 'APPLIANCE' section with 'Settings' and a 'SETUP' section with 'Settings' and 'Upgrade'. The version '4.0.0' is displayed at the bottom of the sidebar. The main content area is titled 'Logs' and shows a dropdown menu with 'authentication.log' selected. To the right of the dropdown are 'Download' and 'Refresh' buttons. The log entries are as follows:

```

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**:

GENERAL

- Endpoints
- User Directories
- Logs
- Status**

APPLIANCE

- Settings

SETUP

- Settings
- Upgrade

Version 4.0.0

Status

All status checks have passed

Connectivity to cloud.logintc.com	Passed
CPU Usage	Passed
RAM Usage	Passed
Disk Space	Passed

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

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

```

Also make sure to check the PostgreSQL logs (`/var/lib/pgsql/data/pg_log`) and secure logs on the Linux machine hosting PostgreSQL (`/var/log/secure`).

Email Support

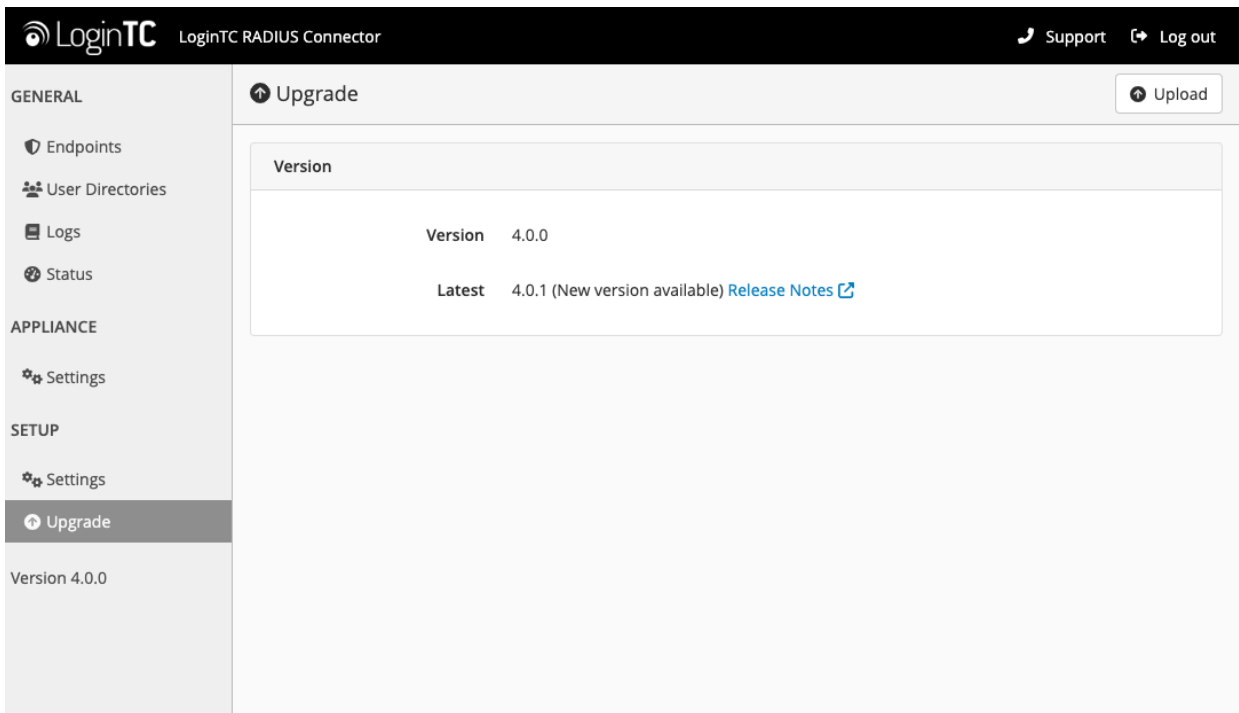
For any additional help please email support@cyphercor.com. Expect a speedy reply.

Upgrading

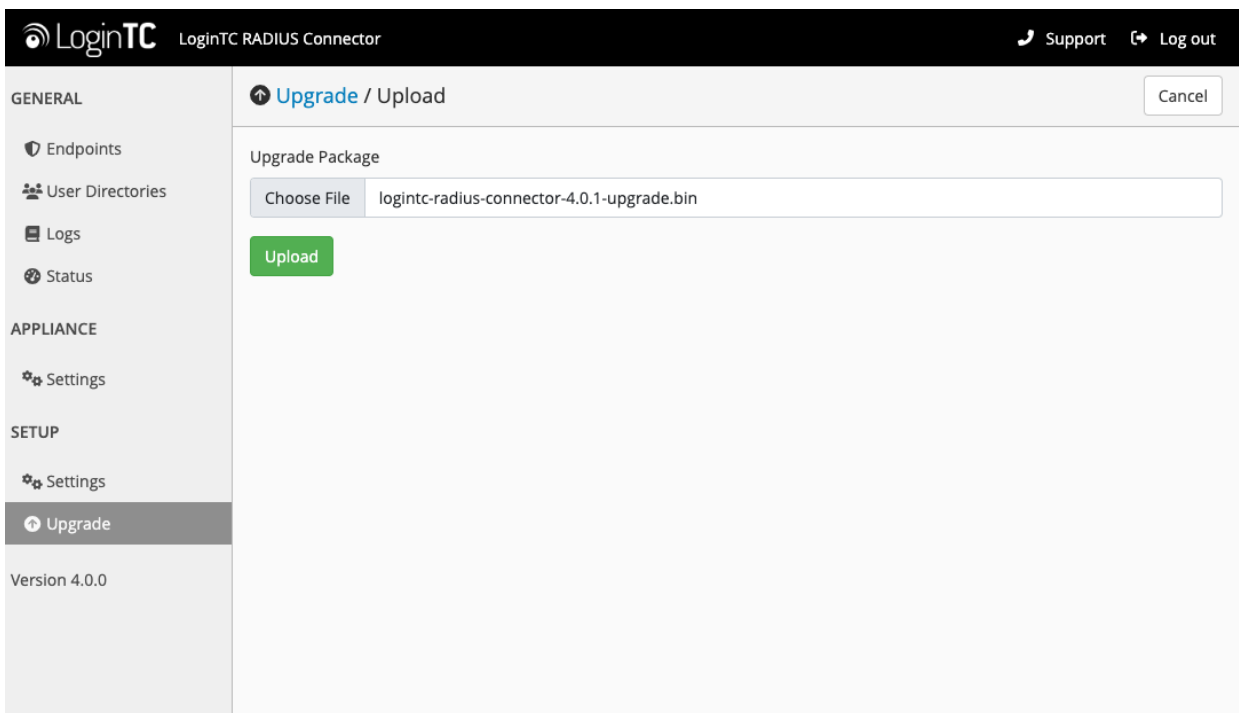
From 4.X

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

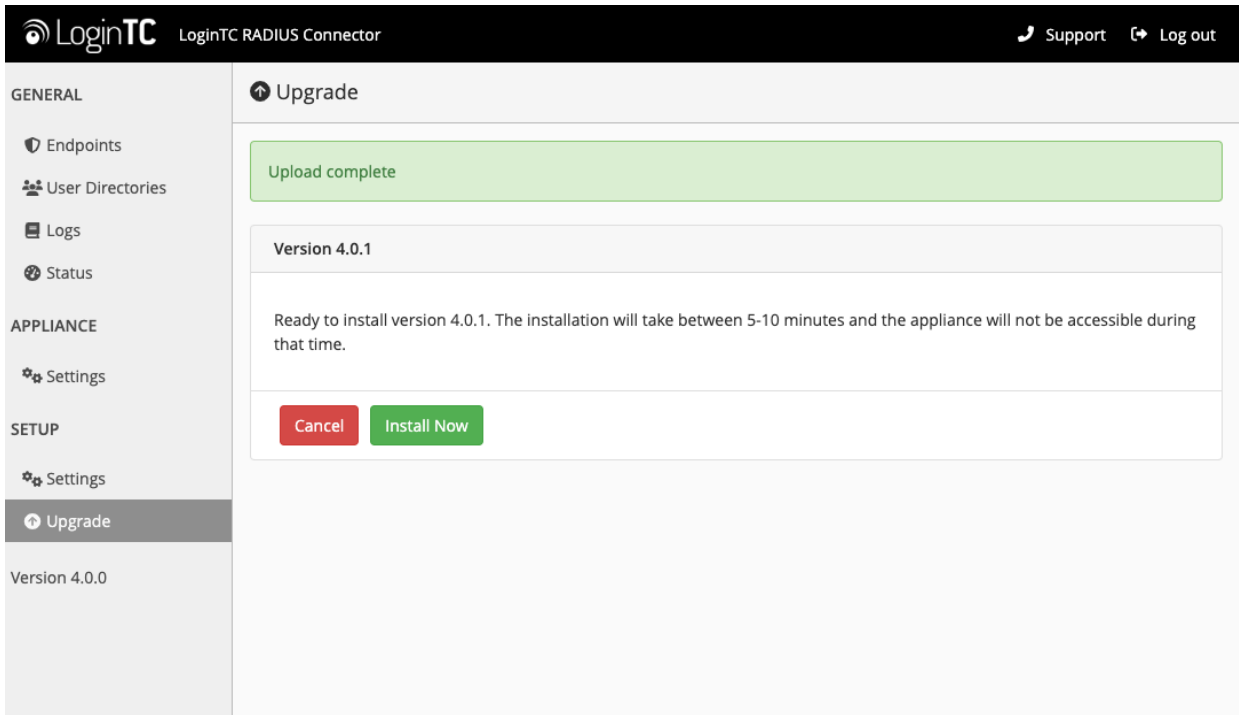
1. Navigate to **SETUP > Upgrade**:



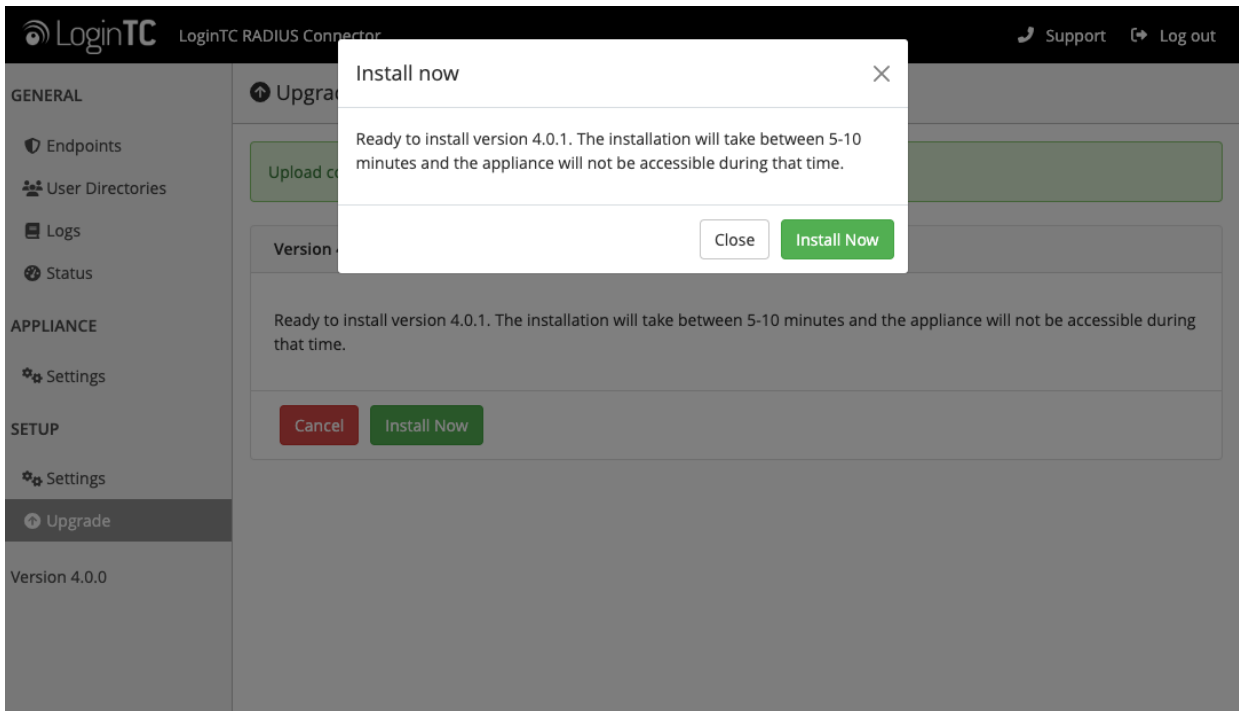
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



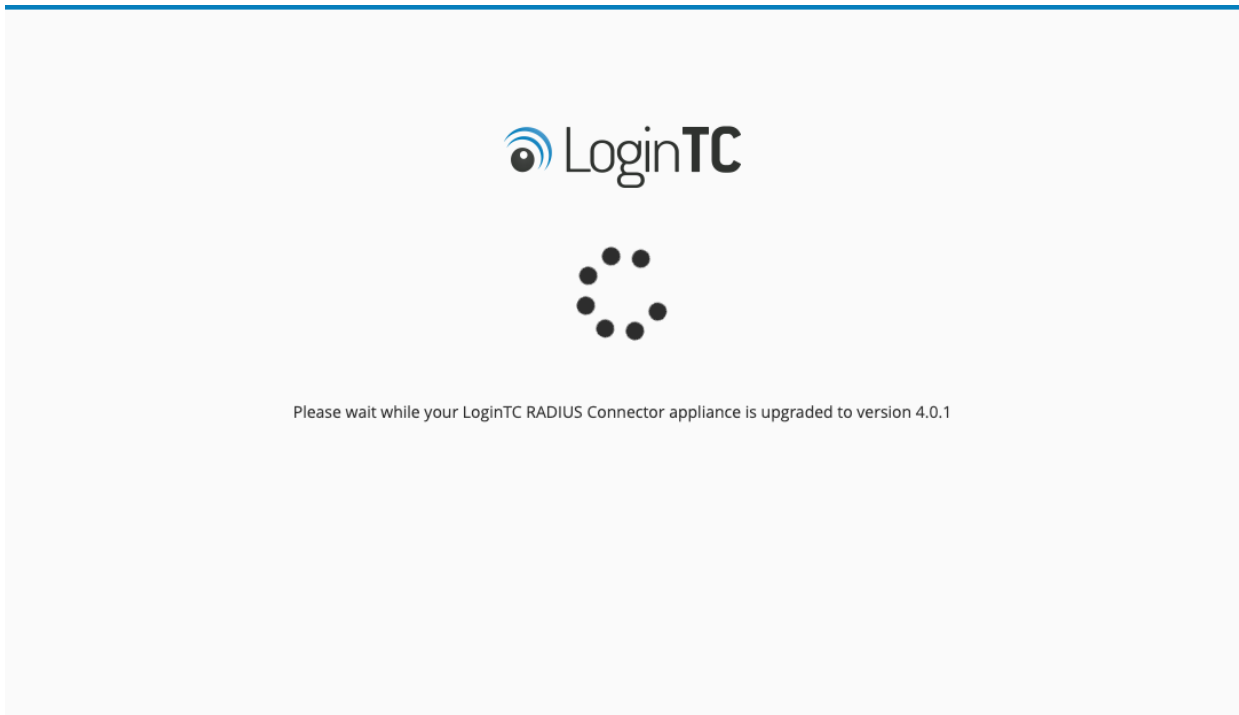
3. Click **Upload** and do not navigate away from the page:



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](#)