

F5 BIG-IP APM Two-Factor Authentication (2FA)

logintc.com/docs/connectors/f5

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables F5 BIG-IP APM to use LoginTC for the most secure two-factor authentication.

Subscription Requirement

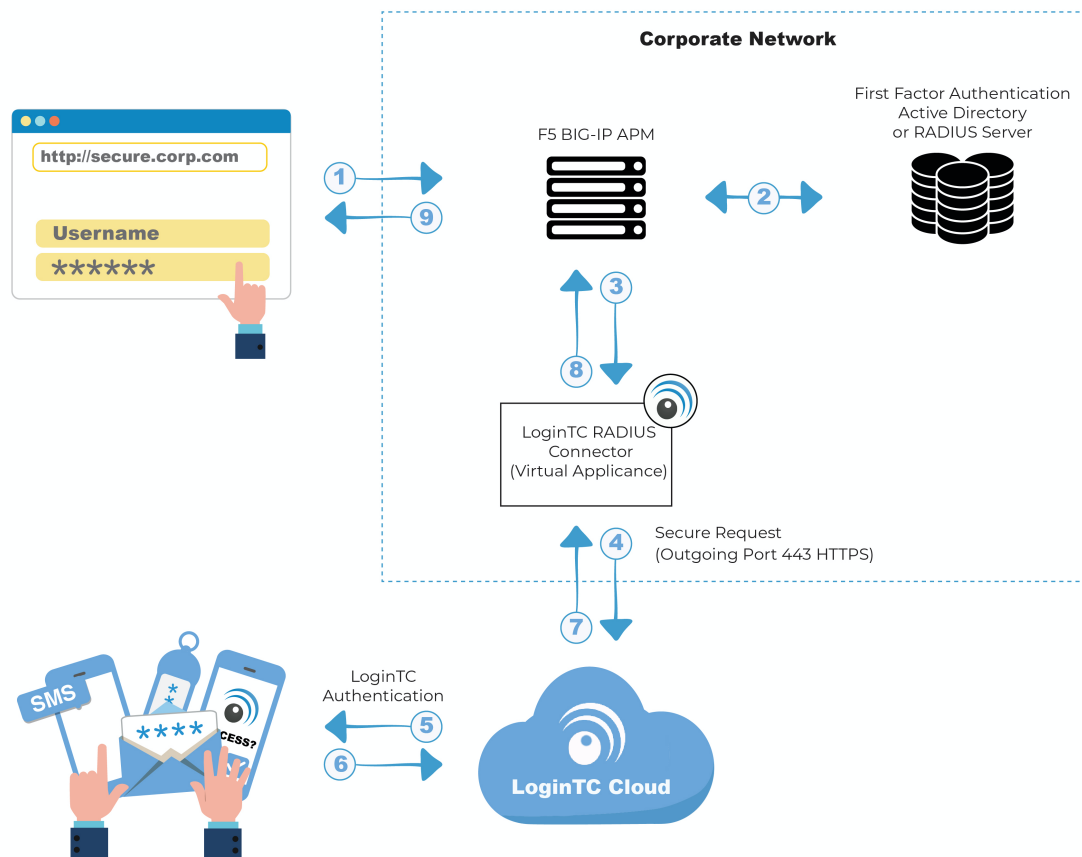
Your organization requires the **Business** or **Enterprise** plan to use the Iframe mode of the LoginTC RADIUS Connector. See the Pricing page for more information about subscription options.

User Experience

There are a wide variety of authentication mechanism users can use to perform MFA with the F5 BIG-IP APM product suite.

Watch Video At: <https://youtu.be/zBwoKz-SXml>

Architecture



Authentication Flow

1. A user attempts access with username / password
2. The username / password is verified against an existing first factor directory (LDAP, Active Directory or RADIUS)
3. A RADIUS authentication request is sent to the LoginTC RADIUS Connector
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 F5
9. User is granted access to F5

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

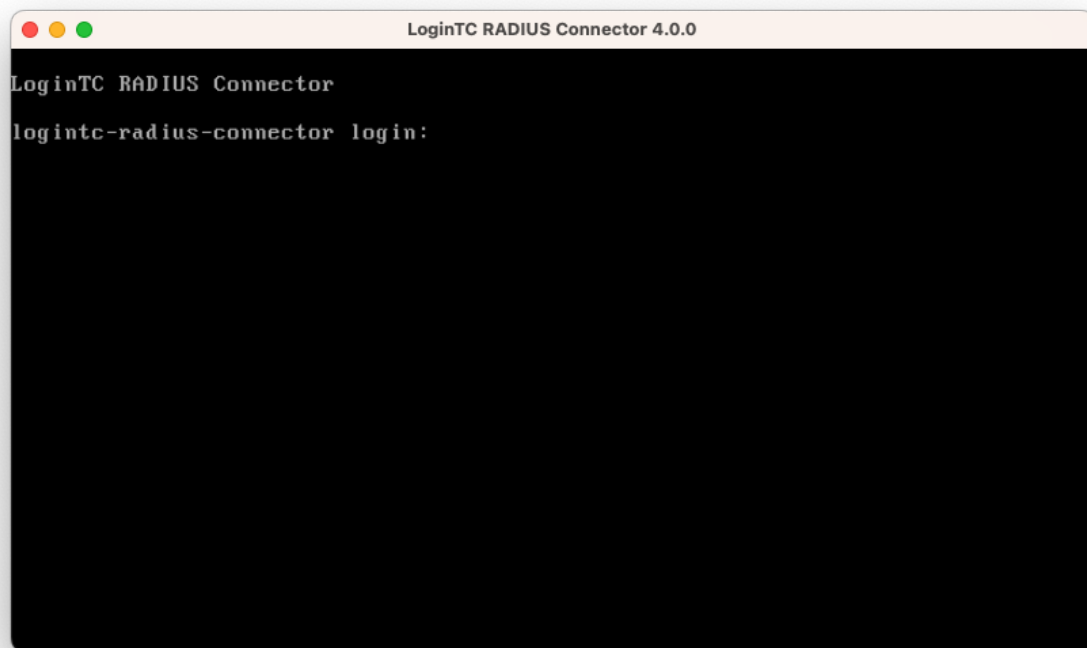
Start by creating a LoginTC Application for your deployment. An Application represents a service (e.g. An application is a service (e.g., VPN or web application) that you want to protect. e) that you want to protect with LoginTC.

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

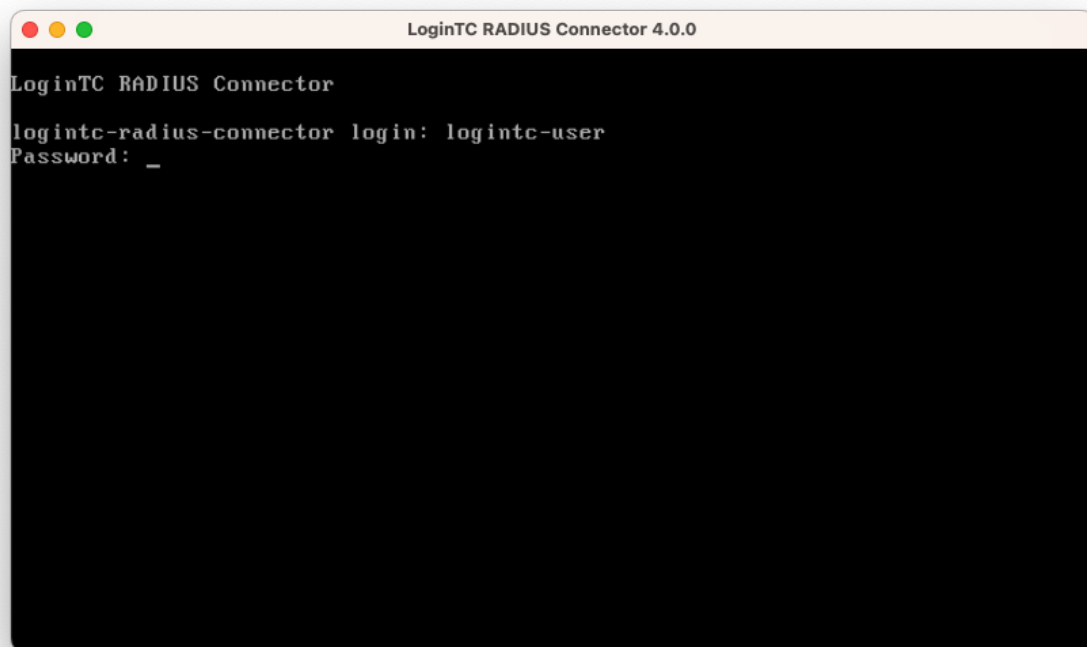
If you have already created a LoginTC Application for your deployment, then you may skip this section and proceed to [Installation](#).

Installation

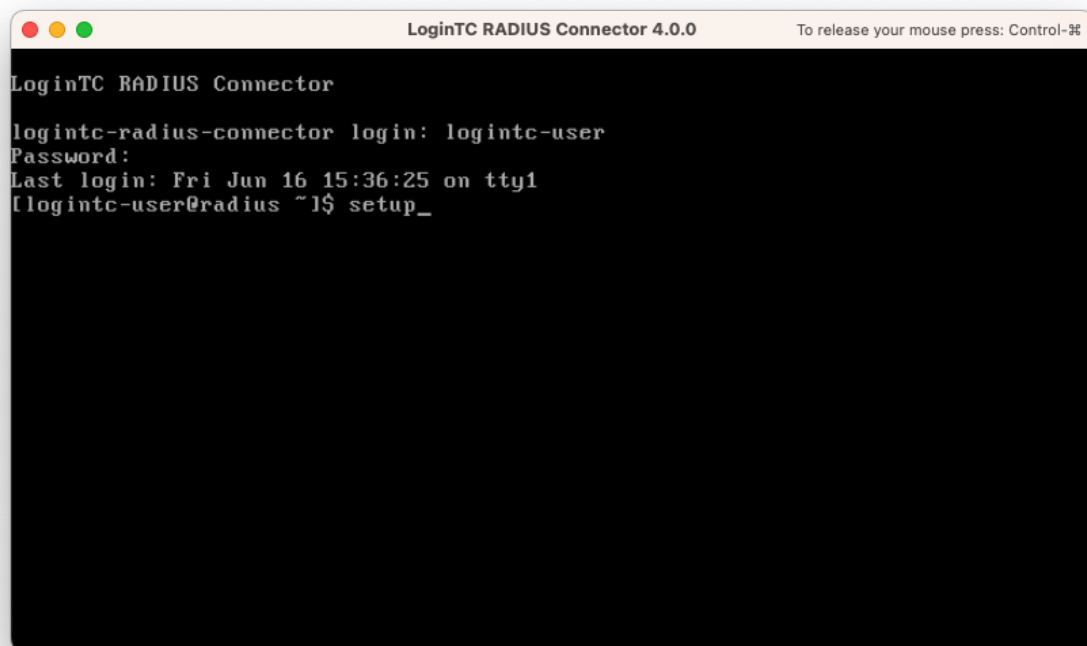
1. Import the virtual appliance your computer virtualization software
[Instructions for Hyper-V](#)
2. Ensure that LoginTC RADIUS CONNECTOR has a virtual network card
3. Start the virtual appliance
4. You will be with a console prompt:



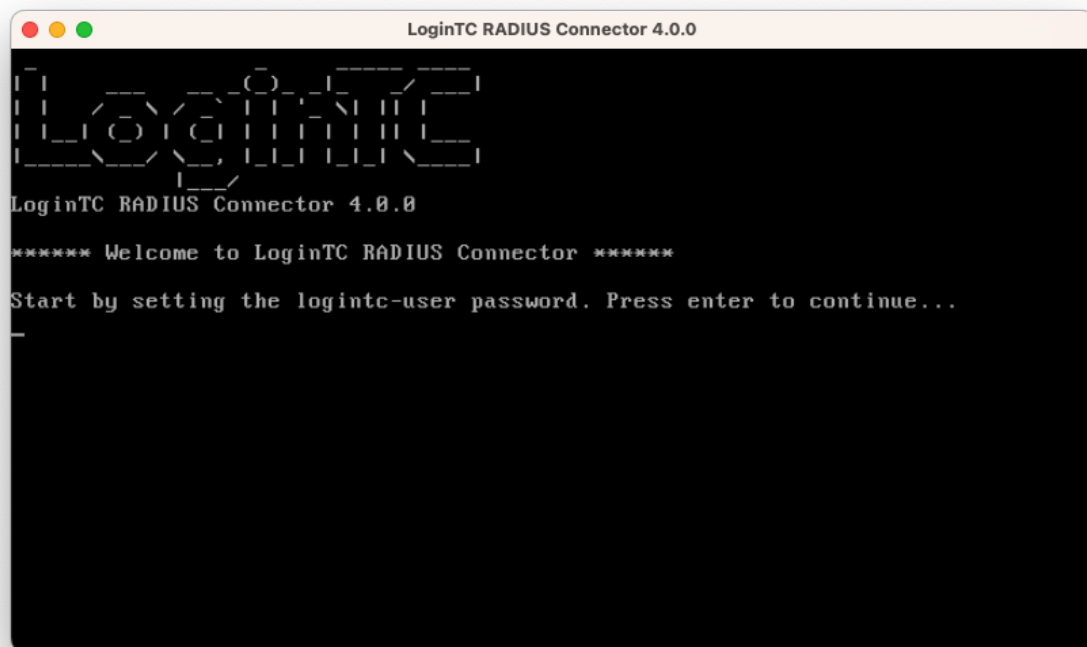
5. Login using the username **logintc-user** and default password **logintcradius**:



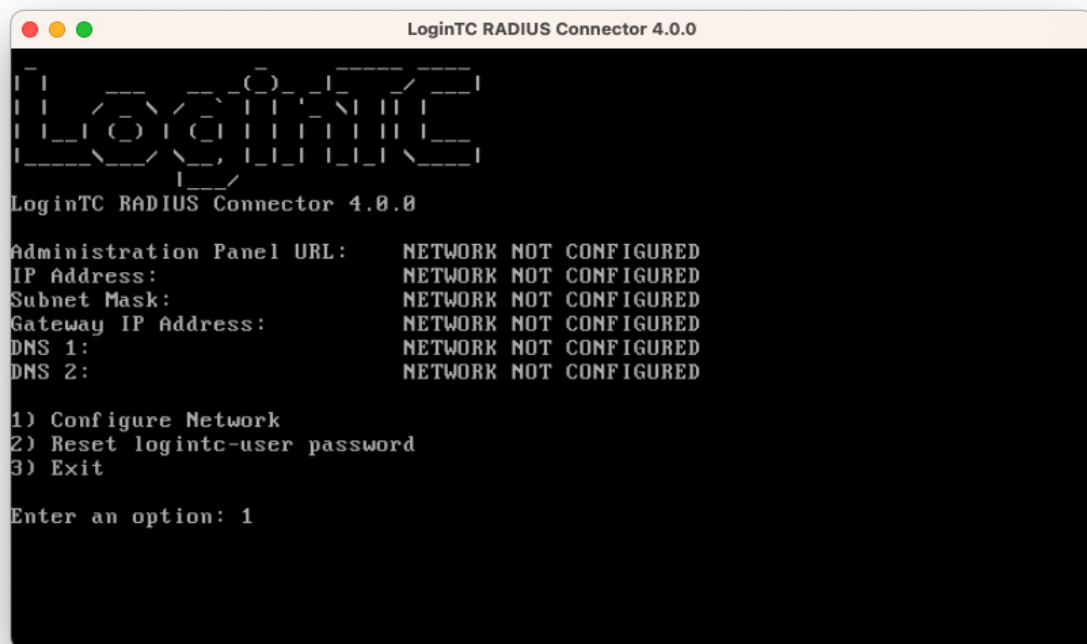
6. Once logged in type **setup**:



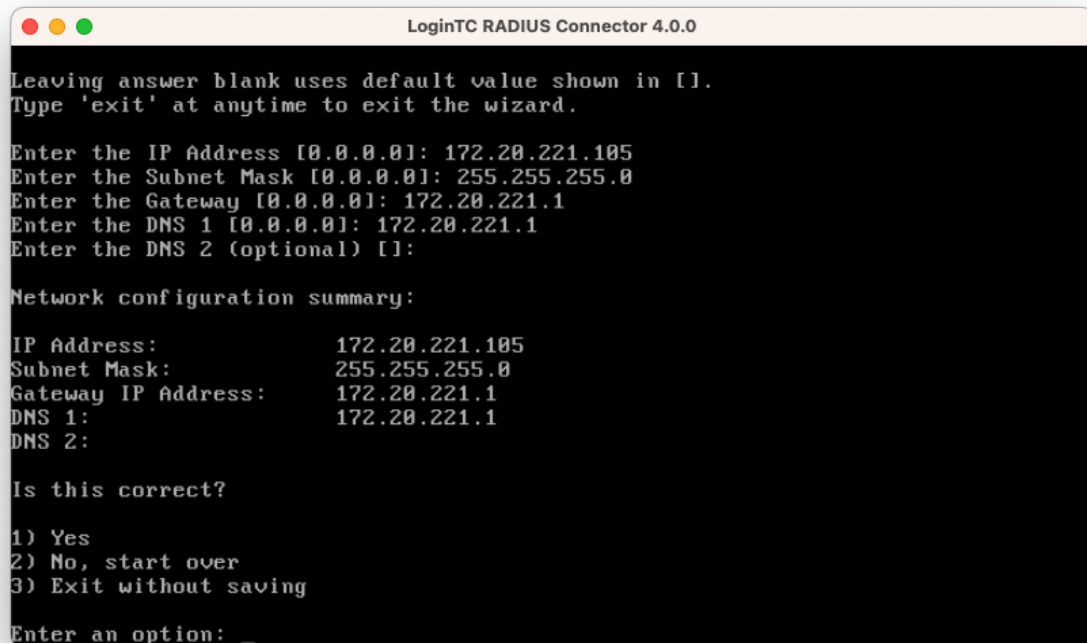
7. Follow the on-screen prompt to setup a new password for **logintc-user**:



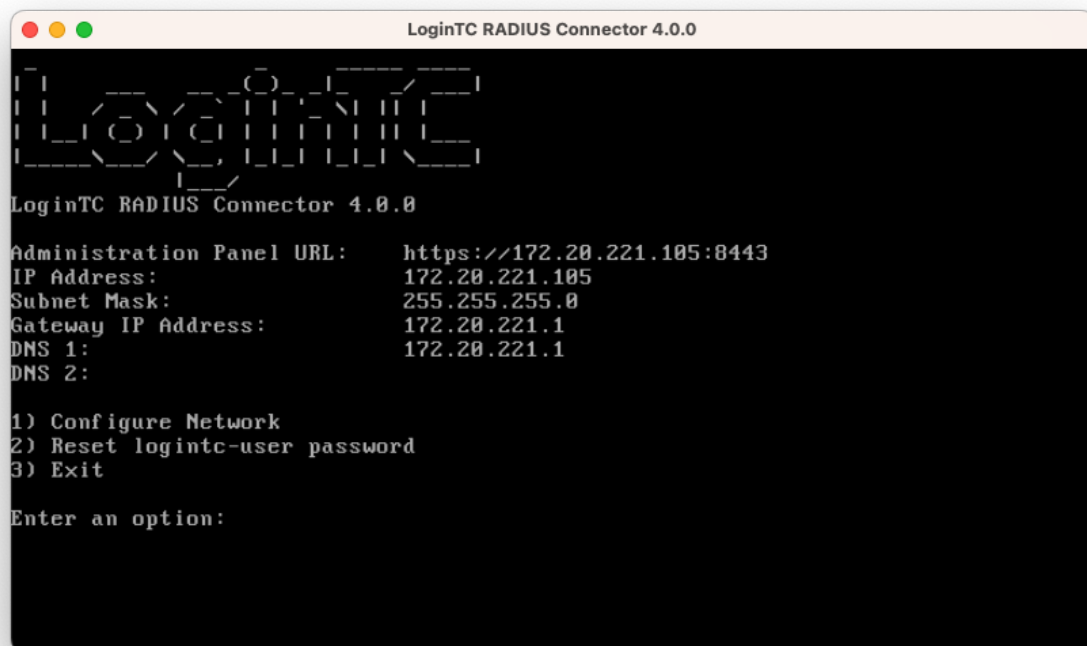
8. By default the appliance network is not configured. Manually configure the network by typing **1** and hit enter:



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



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>):



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

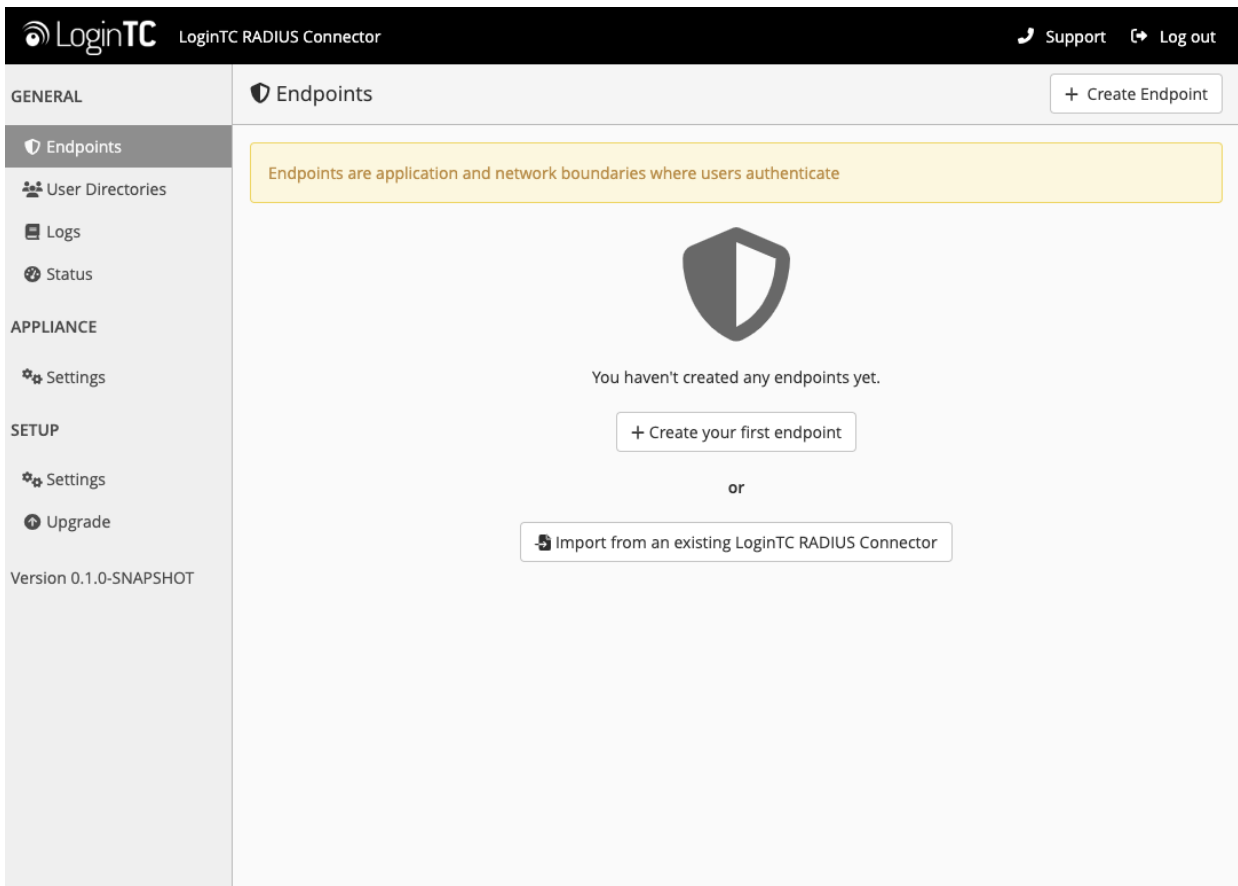
No, continue to the administration panel

[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 F5 MFA

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 / Create / LoginTC Application

Step 1 of 4

Cancel

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings


SETUP

Settings

Upgrade

Version 4.0.0


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:

15/49

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, 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

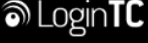
The Application ID and Application API Key are found on the [LoginTC Admin Panel](#).

Request Timeout

16/49

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

SupportLog out

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings


Upgrade

Version 4.0.0

Endpoints / Create / User Directory

Step 2 of 4BackCancel

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**:

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)

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.

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 shows "Step 3 of 4". It includes a yellow instruction box: "Select which users should be challenges with LoginTC and which should bypass LoginTC". Below this are three options: "Challenge All Users" (with a checkmark icon and description "All users will be challenged with LoginTC."), "Challenge Users Based on Static Username List" (with a document icon and description "Only users in a static username list will be challenged with LoginTC."), and "Challenge Users Based on Group Membership" (with a group of people icon and 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'. On the left, a sidebar menu shows 'GENERAL' (selected), 'Endpoints', 'User Directories', 'Logs', 'Status', 'APPLIANCE' (Settings), and 'SETUP' (Settings, Upgrade). The main panel 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 has a large text input field. Below it, a note states: 'Enter a newline separated list of usernames that will be challenged with LoginTC. Users not in this list will bypass LoginTC. Example:'. Below the note is a text area containing the example usernames: 'jane.doe', 'jane.smith', 'john.doe', and 'john.smith'. At the bottom of the main panel, there are 'Test' and 'Next' buttons, and a yellow warning box that 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.

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 main content area is titled 'Endpoints / Create / Challenge Strategy' and indicates 'Step 3 of 4'. On the left, a sidebar menu lists 'GENERAL' (with sub-items: Endpoints, User Directories, Logs, Status) and 'APPLIANCE' (with sub-items: Settings). The main panel is divided into two sections: 'Group Membership' and 'Challenge Groups'. The 'Group Membership' section contains the text: 'Precedence is always given to bypass groups when both challenge and bypass groups are specified.' The 'Challenge Groups' section has a text input field and the instruction: 'Comma separated list of groups whose users will be challenged with LoginTC. Example: 2FA Users'. Below this is the 'Bypass Groups' section, also with a text input field and the instruction: 'Comma separated list of groups whose users will always bypass LoginTC. Example: No 2FA Users'. At the bottom of the main panel, there are 'Test' and 'Next' buttons, and a yellow warning box that 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 plus .	192.168.1.44
Shared Secret	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret

Under Authentication Mode select **Iframe**

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

Shared Secret

The RADIUS shared secret.

Authentication Mode

☐ Direct
☒ Iframe
☐ Challenge
☐ Challenge Interactive

How the LoginTC authentication is performed

A LoginTC iframe will be presented to the user. This is only used for select RADIUS clients with a web-based user interface.

Normalize Usernames

☒ No
☐ Yes, normalize usernames

Specify whether usernames like "DOMAIN\john.doe" and "john.doe@example.com" are treated as-is or as simply "john.doe"

Usernames will be treated as-is.

Enable Monitoring User

☒ No
☐ Yes, enable a monitoring user

Specify a username that will not require LoginTC

Do not enable monitoring user.

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**.

LoginTC RADIUS Connector

Support
Log out

GENERAL

Endpoints

+ Create Endpoint

Endpoints
User Directories
Logs
Status

APPLIANCE
Settings

SETUP
Settings
Upgrade
Version 4.0.0

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**

The screenshot shows the LoginTC Admin Panel interface. The top header is blue and contains the LoginTC logo, the text "Example Inc. Business", and links for "Docs", "Support", and a user profile for "administrator@example.com". The left sidebar is grey and contains 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 (highlighted), Administrators, and Admin Logs. The main content area is white and titled "Domains / Example Inc. Secure Access". It features three buttons: "+ Create Member", "Members", and "Settings". The "Members" section shows "Example Inc. Secure Access has 88 member(s)" and buttons for "+ Create Member" and "View Members". The "Attributes" section states "Example Inc. Secure Access doesn't have any domain attributes yet. [Learn more.](#)" and includes a "+ Create Domain Attribute" button. The "Latest Actions" section displays a table of recent 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' and includes a '+ Create Member' button and a 'Settings' gear icon. Below the title are filters for 'State' (Any) and 'Filter', and a search bar. There are three buttons: 'Issue New Token' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). A message says 'Perform bulk action on 0 selected users'. A table lists users with columns: 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' and includes a '+ Create Member' button and a 'Settings' gear icon. Below the title are filters for 'State' (Any) and 'Filter', and a search bar. There are three buttons: 'Issue New Token' (green), 'Revoke Token' (red), and 'Remove from Domain' (red). A message says 'Perform bulk action on 0 selected users'. A table lists users with columns: Username, State, Activation Code, and Actions. The user 'john.doe' is listed with a state of 'Pending' and an activation code 'HURRMUGUVH'. The Actions column contains a red 'Revoke Token' button.

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 with white text has three buttons: "Cancel", "Add Token", and "Next". The main content area has a light gray background. It features a title "Step 1 of 3: Enter Activation Code" in bold. 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 visible with four rows of keys: the first row has Q, W, E, R, T, Y, U, I, O, P; the second row has A, S, D, F, G, H, J, K, L; the third row has an arrow key, Z, X, C, V, B, N, M, and a delete key; the fourth row has a "123" key, a globe icon, a microphone icon, a "space" key, and a "Next" button.

No SIM 2:28 PM

Cancel Add Token Next

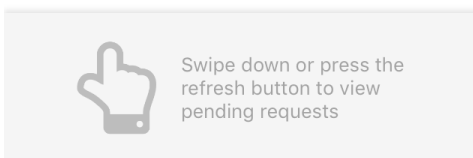
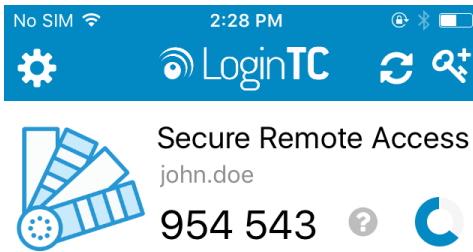
Step 1 of 3: Enter Activation Code

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 RADIUS Connector

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

GENERAL

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Endpoints / Generic RADIUS

Test EndpointDelete


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

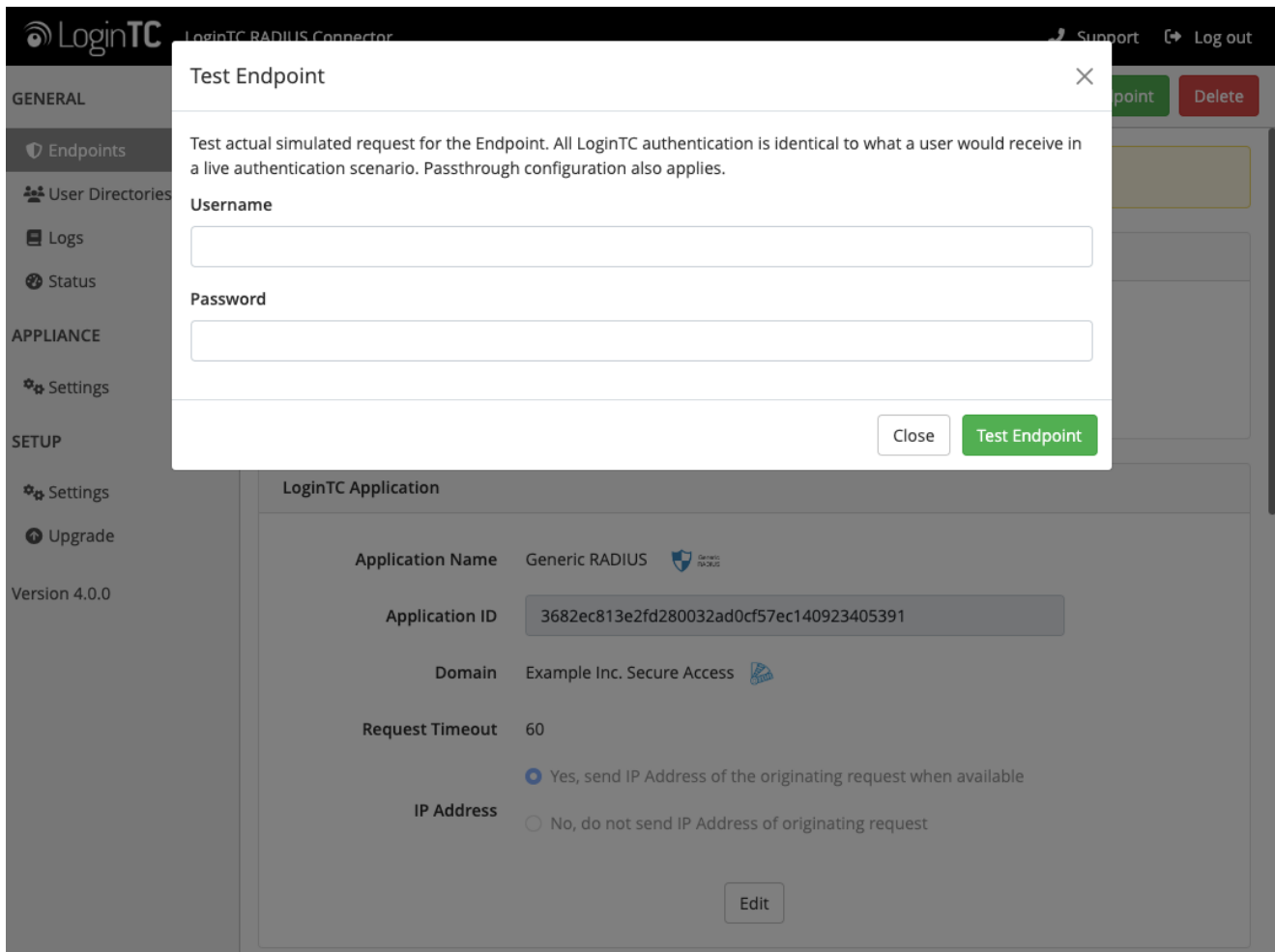
IP Address

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

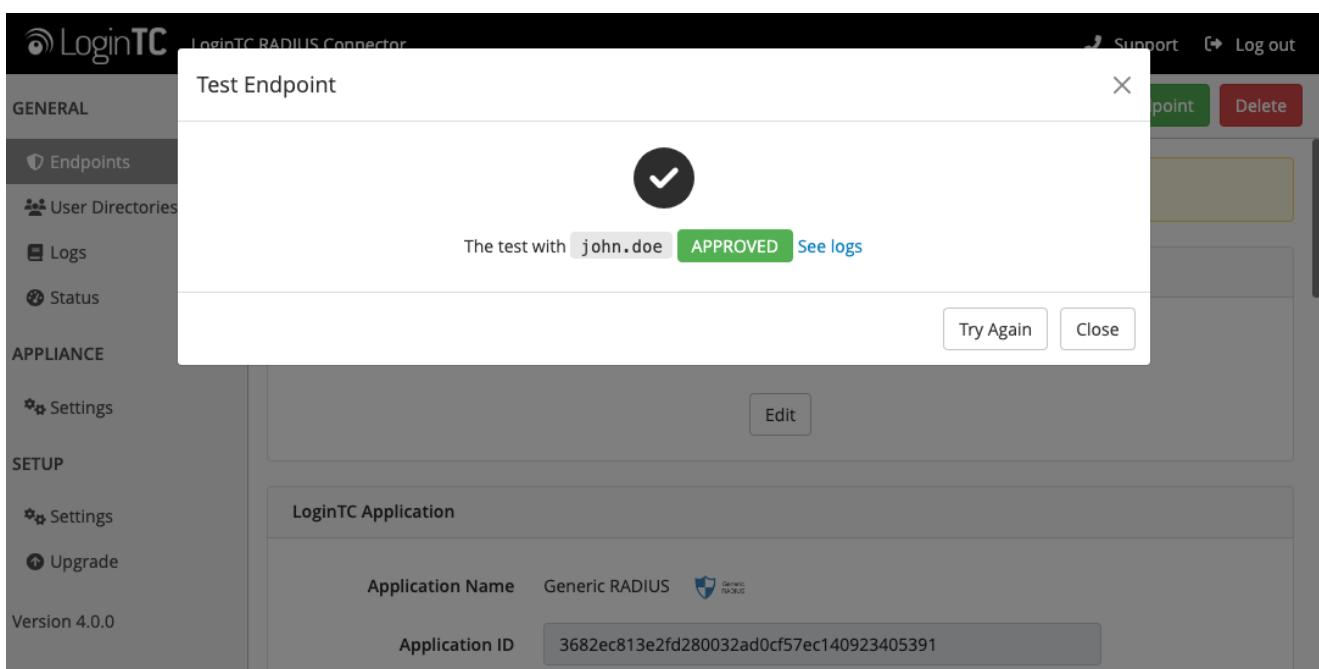
☐ No, do not send IP Address of originating request

Edit

Click **Test Configuration**:

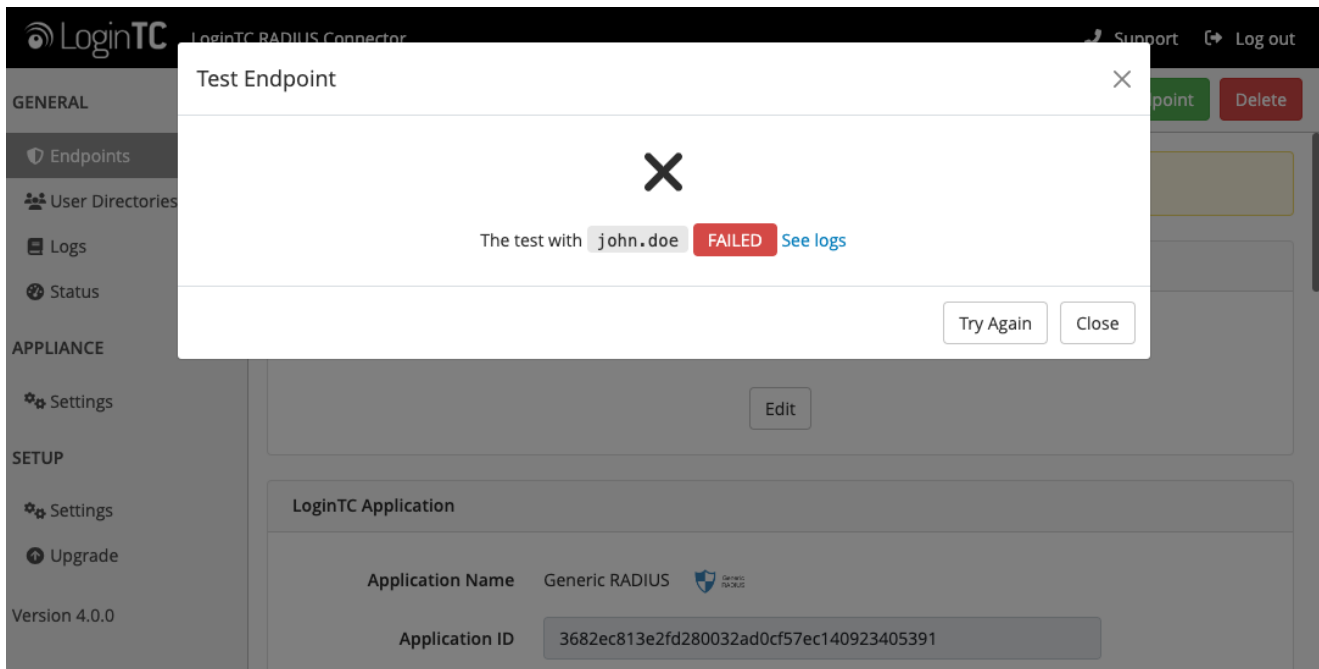


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

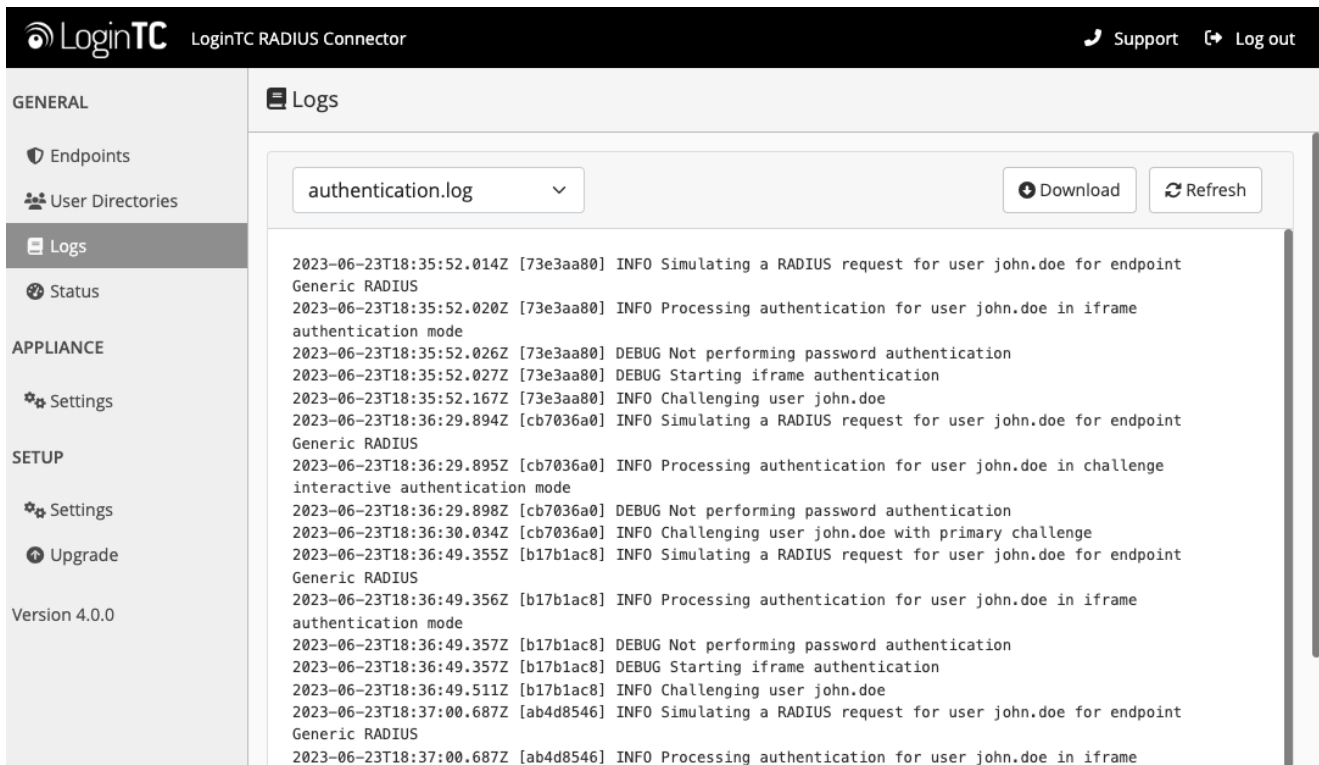


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



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



F5 MFA Configuration

Once you are satisfied with your setup, configure your F5 Big-IP APM 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. A left sidebar contains navigation links: 'GENERAL' (Endpoints, User Directories, Logs, Status), 'APPLIANCE' (Settings), and 'SETUP' (Settings, Upgrade). The main content area is titled 'Settings' and 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.

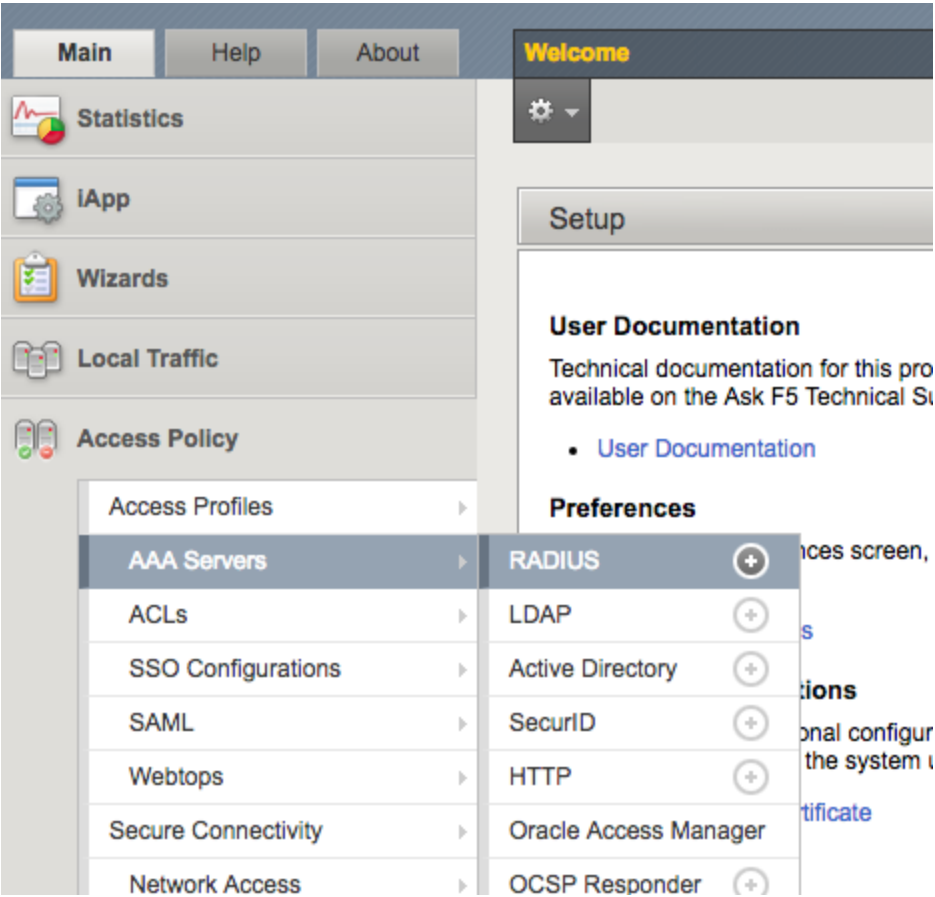
RADIUS Details	
IP Address	172.20.221.85
RADIUS Authentication Port	1812

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 setup F5 Big-IP APM with LoginTC.

1. Log into the F5 Big-IP Configuration Utility / Management Console

2. Navigate to **Access Policy > AAA Servers > RADIUS**:



3. Click **Create...**

General Properties

Name

LoginTC

Type

RADIUS

Configuration

Mode

☒ Authentication
 ☐ Accounting
 ☐ Authentication & Accounting

Server Connection

☐ Use Pool
 ☒ Direct

Server Address

192.168.1.7

Authentication Service Port

1812

Secret

.....

Confirm Secret

.....

NAS IP Address

NAS IPV6 Address

NAS Identifier

Timeout

90

seconds

Retries

1

Service Type

Default

Cancel

Repeat

Finished

Property	Explanation	Example
Name	The name of this configuration.	LoginTC
Mode	The method in which F5 will leverage the LoginTC RADIUS Connector. Must be Authentication.	Authentication
Server Connection	The type of connection, either Use Pool or Direct. Use Pool can be leveraged for failover scenarios.	Direct
Server Address	Address of your LoginTC RADIUS Connector	192.168.1.7
Authentication Port	RADIUS authentication port. Must be 1812.	1812

Property	Explanation	Example
Secret	The secret shared between F5 and LoginTC RADIUS Connector	bigsecret
Confirm Secret	Confirmation of shared secret between F5 and LoginTC RADIUS Connector	bigsecret
Timeout	Authentication timeout. Recommend 60s and must be larger than the LoginTC request timeout.	60
Retries	Number of times to send authentication request. Must be 1.	1
Service Type	Maximum number of retransmission attempts. Must be Default.	Default

4. Click **Finished**

Access Policy » AAA Servers : RADIUS

⚙️ All AAA Server List AAA Servers By Type

RADIUS Servers

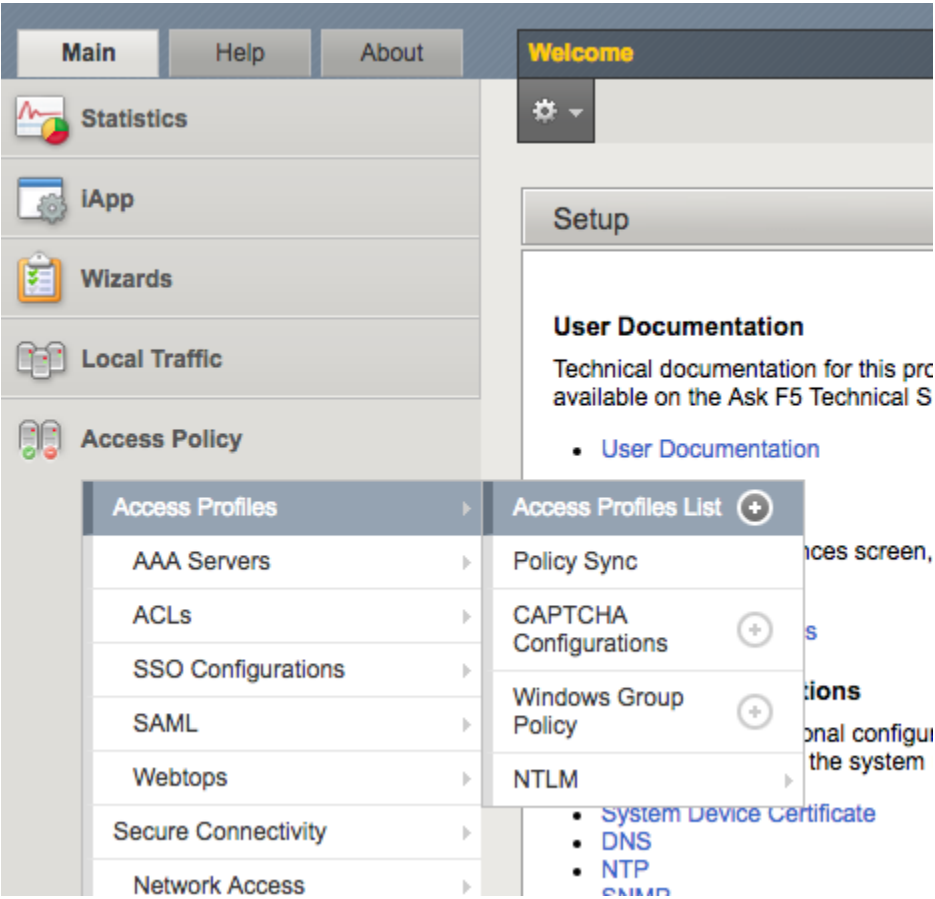
☒ Name

☐ LoginTC

Delete...

5. Modify an existing Access Policy or create an new one to leverage the newly defined RADIUS server pointing to the LoginTC RADIUS Connector.

6. Navigate to **Access Policy > Access Profiles > Access Profiles List:**



7. For the Access Profile you wish to edit click **Edit....**

8. To add the LoginTC RADIUS server click on the appropriate **+** link, select **RADIUS Auth*** and click **Add Item**:

The screenshot shows the F5 BIG-IP configuration interface. On the left, the 'Access Policy: /Common' configuration page is visible, showing a 'Start' macro and a 'Logon Page' macro connected by a 'fallback' link. Below this, there is an 'Add New Macro' button and some explanatory text. On the right, the 'Add New Macro' dialog box is open, displaying a list of authentication methods. The 'Authentication' section is expanded, and 'RADIUS Auth' is selected. The dialog box has 'Cancel' and 'Add Item' buttons at the bottom.

Option	Description
<input type="radio"/> Logging	Log custom messages and session variables for reporting and troubleshooting
<input type="radio"/> Message Box	Create a custom message to display to the end user with prompt to continue
<input type="radio"/> Dynamic ACL	Assignment of Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP
<input type="radio"/> Empty	Creates an Empty Action for constructing custom Branch Rules
Authentication	
<input type="radio"/> AD Auth	Active Directory authentication of end user credentials
<input type="radio"/> Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
<input type="radio"/> HTTP Auth	HTTP authentication of end user credentials
<input type="radio"/> LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions / Group Mapping
<input type="radio"/> OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
<input checked="" type="radio"/> RADIUS Auth	RADIUS authentication of end user credentials

Cancel Add Item

9. Fill in the configuration details and click **Save**:

Access Policy: /Common/direct

Edit Ending

Start

fallback

+

Logon Page

×

fallback

+

LoginTC RADIUS A

Add New Macro

An access policy consists of a start point, actions, and one or more actions. Click the **Add Macro** button to add a purpose-built set of predefined macros.

You can get started with [Device Wizards](#). On the main navigation pane, click **Configuration Guide for BIG-IP Access Policy Manager** for more information.

Please see the [Online Help](#) for more Visual Policy Editor basics.

Properties

Branch Rules

Name: LoginTC RADIUS Auth

RADIUS

AAA Server

/Common/LoginTC

Show Extended Error

Disabled

Max Logon Attempts Allowed

1

Cancel

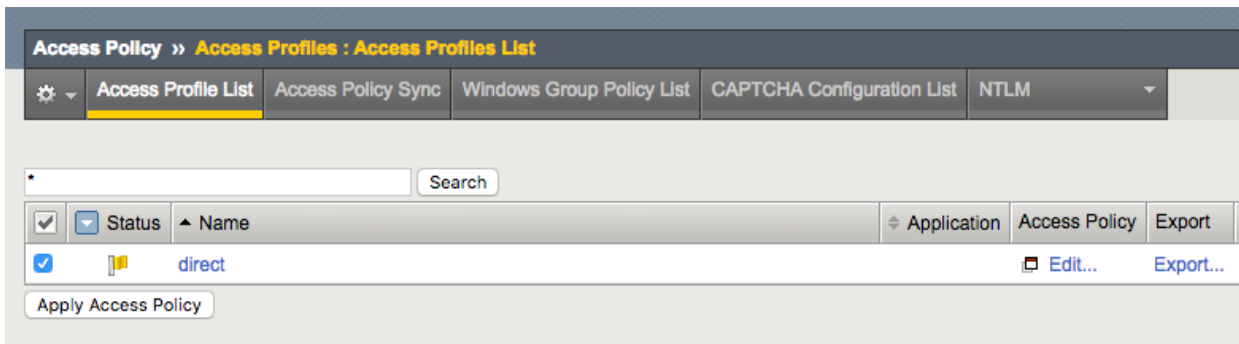
Save

Property	Explanation	Example
Name	The name of this Access Policy Item.	LoginTC RADIUS Auth
AAA Server	The AAA Server to leverage. Must be the one created in Step 3.	LoginTC
Show Extended Error	Displays comprehensive error messages generated by the authentication server. Must be Disabled.	Disabled
Max Logon Attempts Allowed	Number of attempts a user has.	3

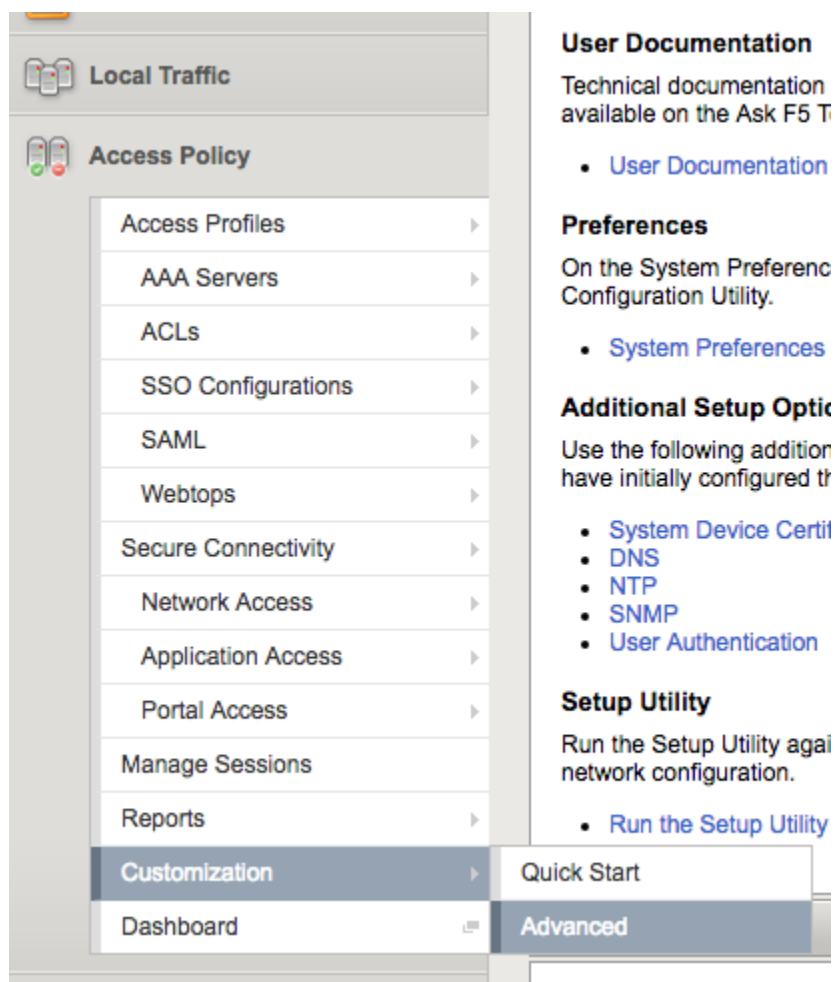
10. Click **Close**

39/49

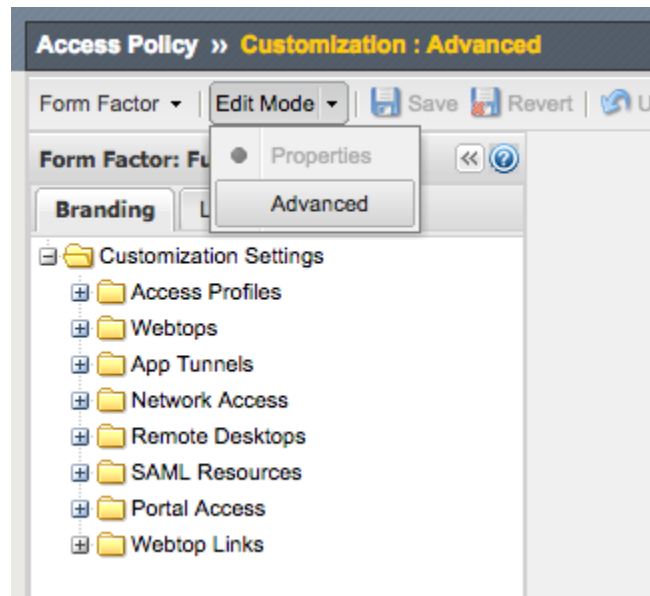
11. On the Access Profiles List the profile just modified will be flagged with a yellow flag. Select it and click **Apply Access Policy**.



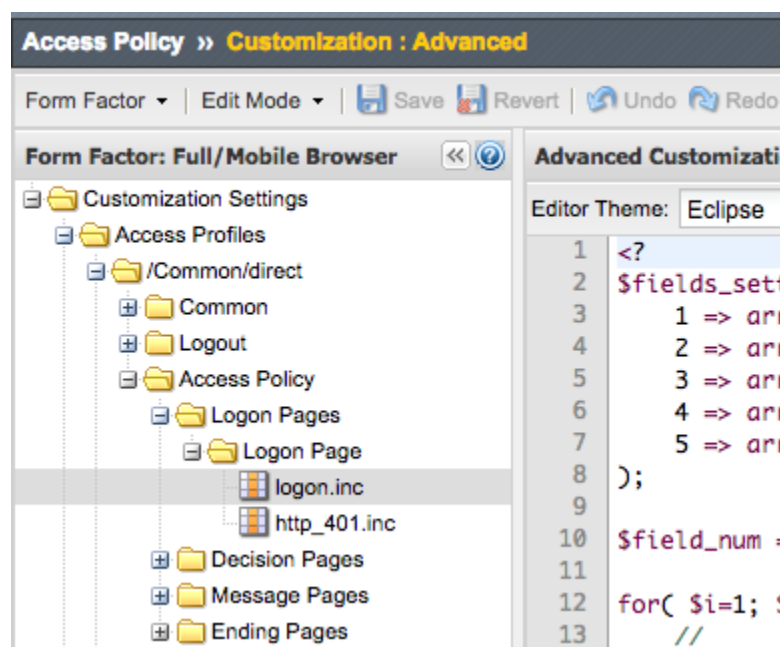
12. Navigate to **Access Policy > Customization > Advanced**:



13. Under **Edit Mode**, select **Advanced**:



14. Find **logon.inc** under **Customization Settings > Access Profiles > [Your Profile Name] > Access Policy > Logon Pages > Logon Page**:



15. Find the line (you use **CTRL F** and search for **</head>**):

```
358
359 </head>
360
```

16. Edit the following snippet with your **Application ID** (<https://www.logintc.com/downloads/f5-code-snippet-v1-app.txt>):

```

<!-- Start of LoginTC F5 Integration -->
<style type="text/css">.logintc #main_table_info_cell { visibility:
hidden; }</style>
<script type="text/javascript">
    var logintc_host = 'cloud.logintc.com';
    var logintc_application_id = 'YOUR_APPLICATION_ID';

    document.documentElement.className="logintc";var
domReady=function(e,n,t){n=document,t="addEventListener",n[t]?n[t]
("DOMContentLoaded",e):window.attachEvent("onload",e)};domReady(function()
{if(-1!=document.getElementById("credentials_table_header").innerHTML.indexOf("LoginTC
Request-Token")){var e=document.createElement("script");e.src="https://" +
logintc_host + "/static/iframe/f5-iframe-injector-
v2.js",document.getElementsByTagName("head")[0].appendChild(e)}else
document.documentElement.className=""});
</script>
<!-- End of LoginTC F5 Integration -->

```

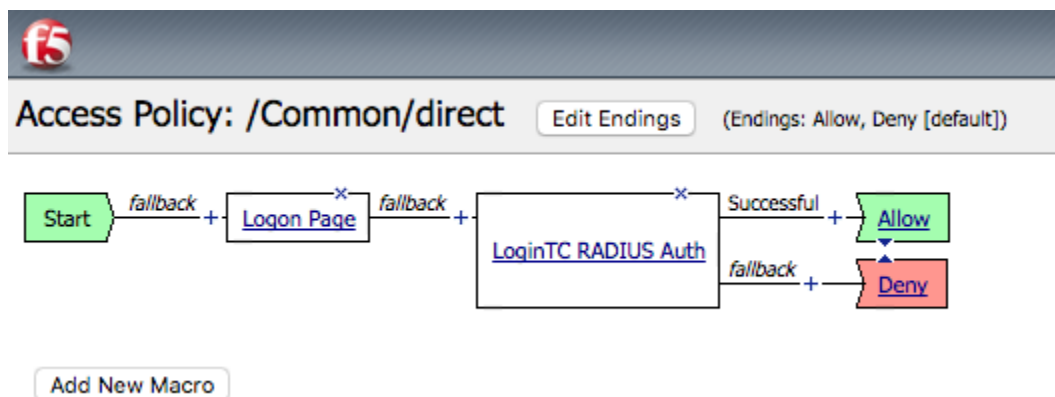
Note: Add your Application ID

Replace **YOUR_APPLICATION_ID** with the actual LoginTC Application ID you wish to use, [retrieve Application ID](#).

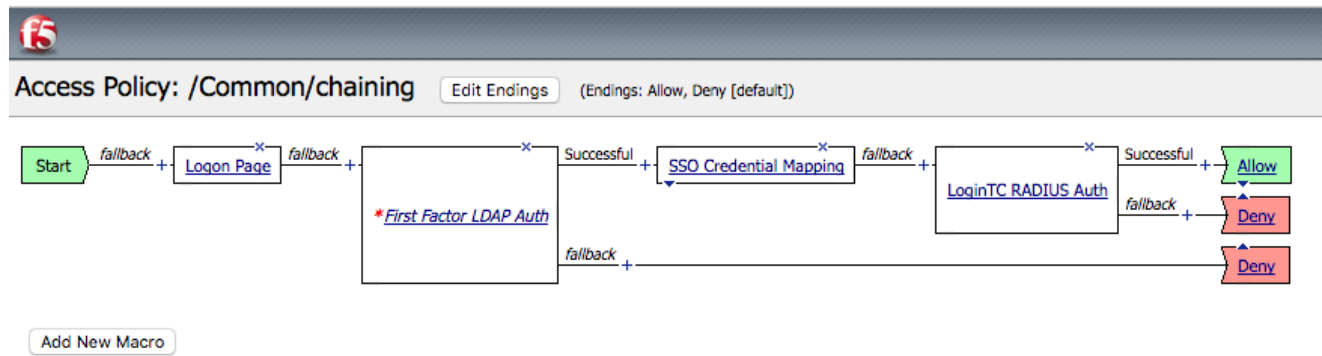
17. Add the edited snippet before **</head>**;
18. Click **Save Draft > Yes > Save**:
19. Navigate to **Access Policy > Access Profiles > Access Profiles List**:
20. On the Access Profiles List the profile just modified will be flagged with a yellow flag. Select it and click **Apply Access Policy**.

There are a variety of ways to add the LoginTC RADIUS Connector to your F5 Access Policy. You can for example replace your existing First Factor authentication, like LDAP / Active Directory with the LoginTC RADIUS Connector. You can also perform First Factor from your existing LDAP / Active Directory and then leverage the LoginTC RADIUS Connector. Here are some end state examples:

Replacing an existing First Factor, like LDAP / Active Directory with the LoginTC RADIUS Connector:



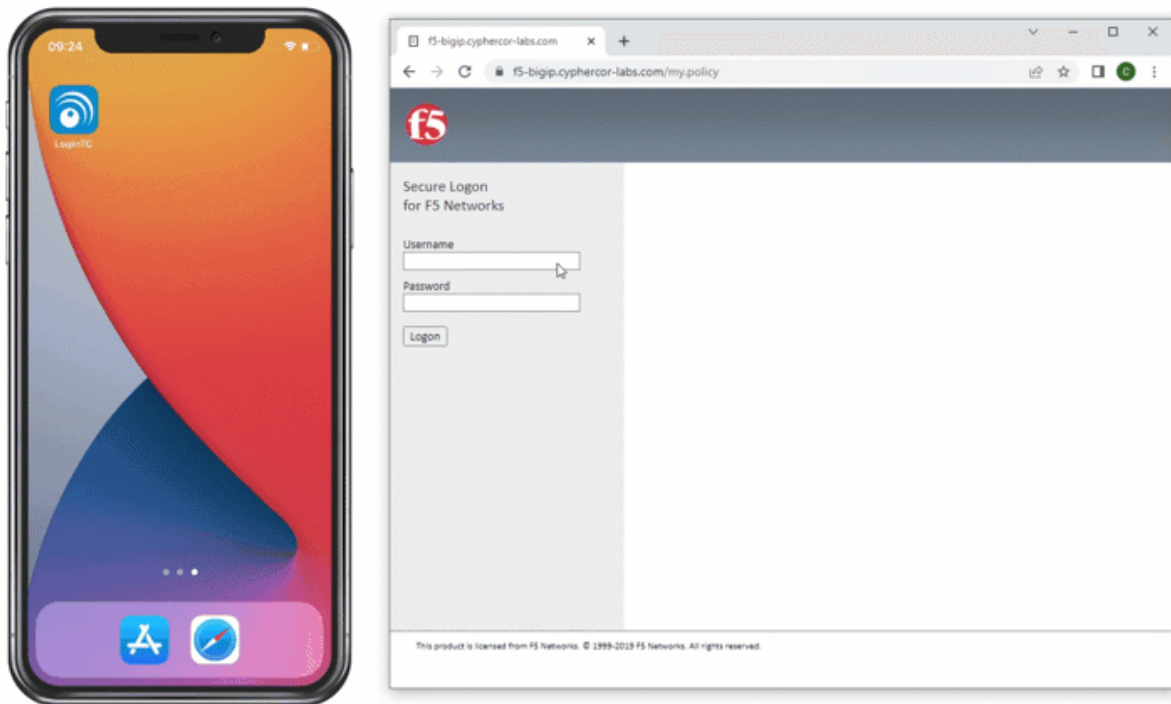
Chaining the LoginTC RADIUS Connector:



To find the way which works best for your environment review the F5 Configuration Guide for BIG-IP Access Policy Manager or contact your F5 vendor or F5 support directly.

F5 Testing

To test, navigate to the logon page using the access policy just configured and attempt to login. You should be prompted with a LoginTC login form:



Select the method you wish to use to authenticate and continue.

Loading Balancing and Health Monitoring

F5 allows for multiple LoginTC RADIUS Connectors to be load balanced for high availability. For more information on how to configure AAA high availability see: [Setting up Access Policy Manager for AAA high availability](#).

Steps to configure a health check monitoring user on the LoginTC RADIUS Connector:

1. From the LoginTC RADIUS Connector web based administration page logon using **logintc-user**
2. Click **Configurations**
3. Click on your configuration
4. Scroll down to **Client Settings** and click **Edit**
5. Monitoring health checks can sometimes originate from an F5 self-ip. Ensure the **IP Address** matches the correct IP Address. May need to create a new configuration dedicated to monitoring if the health check IP Address does not match the IP Address RADIUS authentication calls originate from.
6. Scroll down to **Enable Monitoring User** and select **Yes, enable a monitoring user**

GENERAL

Endpoints / Generic RADIUS / Client Settings / Edit

Cancel

Endpoints

User Directories

Logs

Status

APPLIANCE

Settings

SETUP

Settings

Upgrade

Version 4.0.0

Enable Monitoring User

☐ No ☒ Yes, enable a monitoring user

Specify a username that will not require LoginTC authentication. Use this setting if the device connecting performs monitoring of RADIUS connections and always expects an Access-Accept reply.

Enter the monitoring username.

monitor_user

RADIUS Attributes (Advanced)

☒ None ☐ Specify up to 5 attributes

Do not send any additional RADIUS attributes.

Specify up to 5 attributes (standard or vendor-specific attributes) to be returned to the RADIUS client.

Test Save

7. Enter a **Monitoring Username** that matches the configured **Server Pool Monitor** in F5
8. Click **Test** to validate the values and then click **Save**.

When health checks requests are received for the monitoring user, the configured First Factor authentication will be checked and LoginTC verification will automatically passthrough. If First Factor authentication passes **ACCESS-ACCEPT** will be returned.

LoginTC application dedicated for monitoring

Recommend creating a new LoginTC application and domain only for monitoring. No users need to be part of the application / domain.

(Optional) Active Directory check for monitoring user

Recommend leveraging a dedicated service account for First Factor authentication.

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 the LoginTC Admin is performed using [User Sync Tool](#).

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'. A left sidebar contains a menu with 'GENERAL' (selected), 'Endpoints', 'User Directories', 'Logs' (highlighted), 'Status', 'APPLIANCE' (with 'Settings'), and 'SETUP' (with 'Settings' and 'Upgrade'). The main content area is titled 'Logs' and features a dropdown menu set to 'authentication.log', along with 'Download' and 'Refresh' buttons. The log entries show a sequence of events for user 'john.doe' at endpoint 'Generic RADIUS', including simulated requests, processing in iframe and challenge modes, and debugging messages for password authentication and challenge starting.

Timestamp	Endpoint	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

Not Authenticating

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

LoginTC RADIUS Connector

Support
Log out

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**:

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

```

Email Support

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

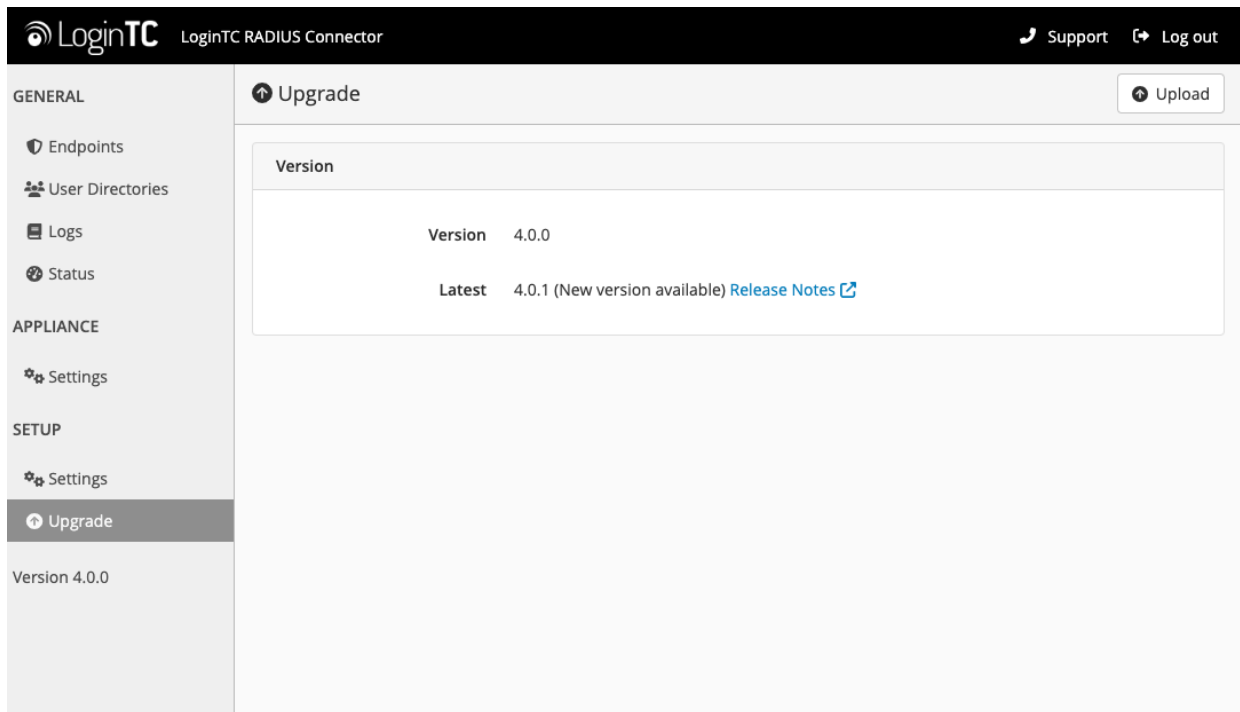
Upgrading

46/49

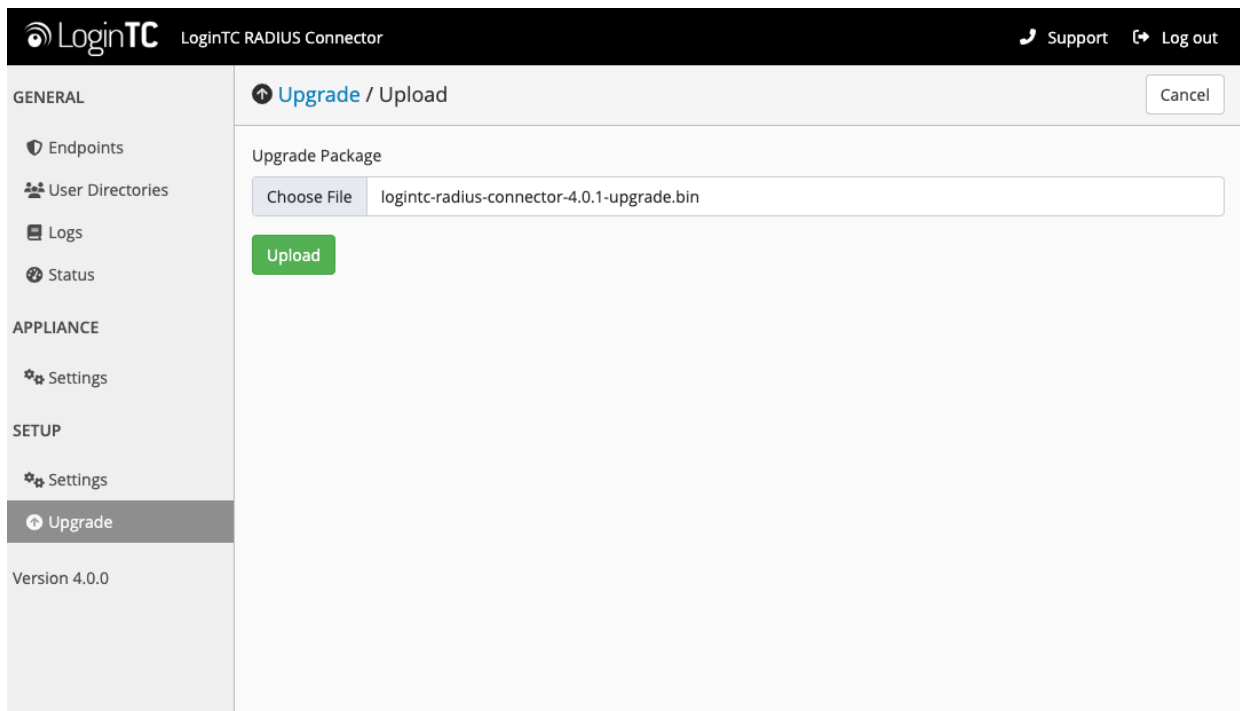
From 4.X

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

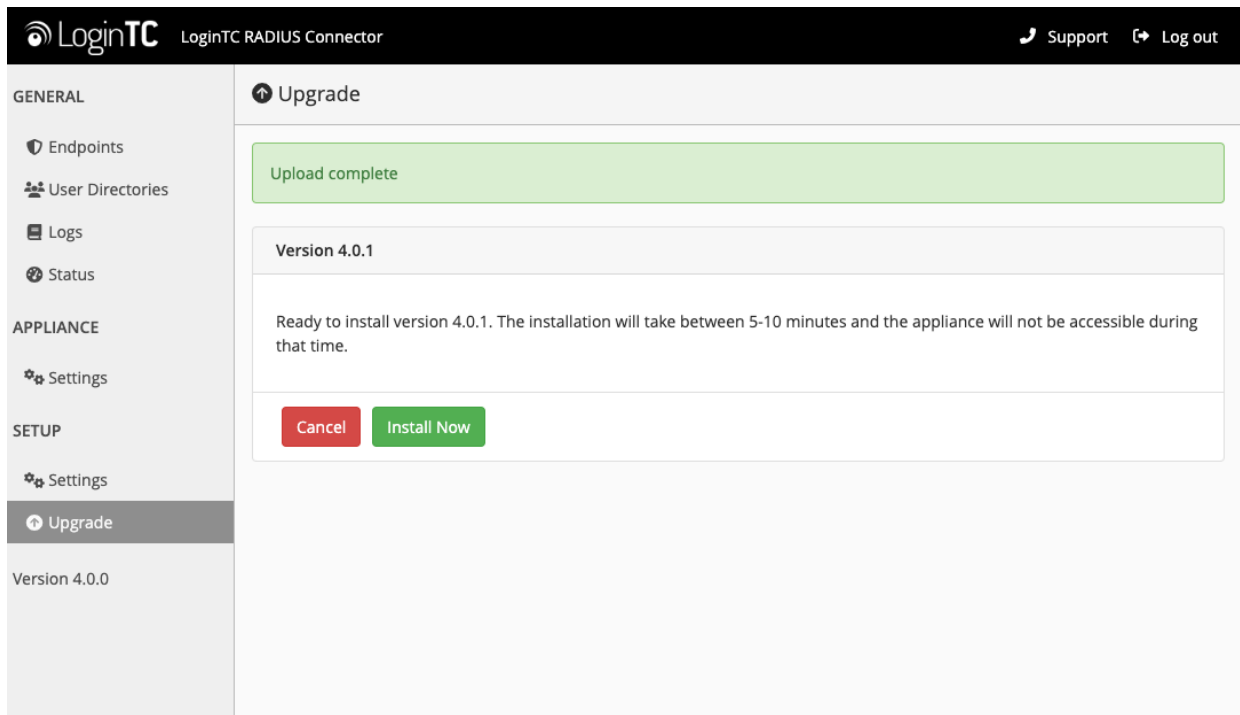
1. Navigate to **SETUP > Upgrade**:



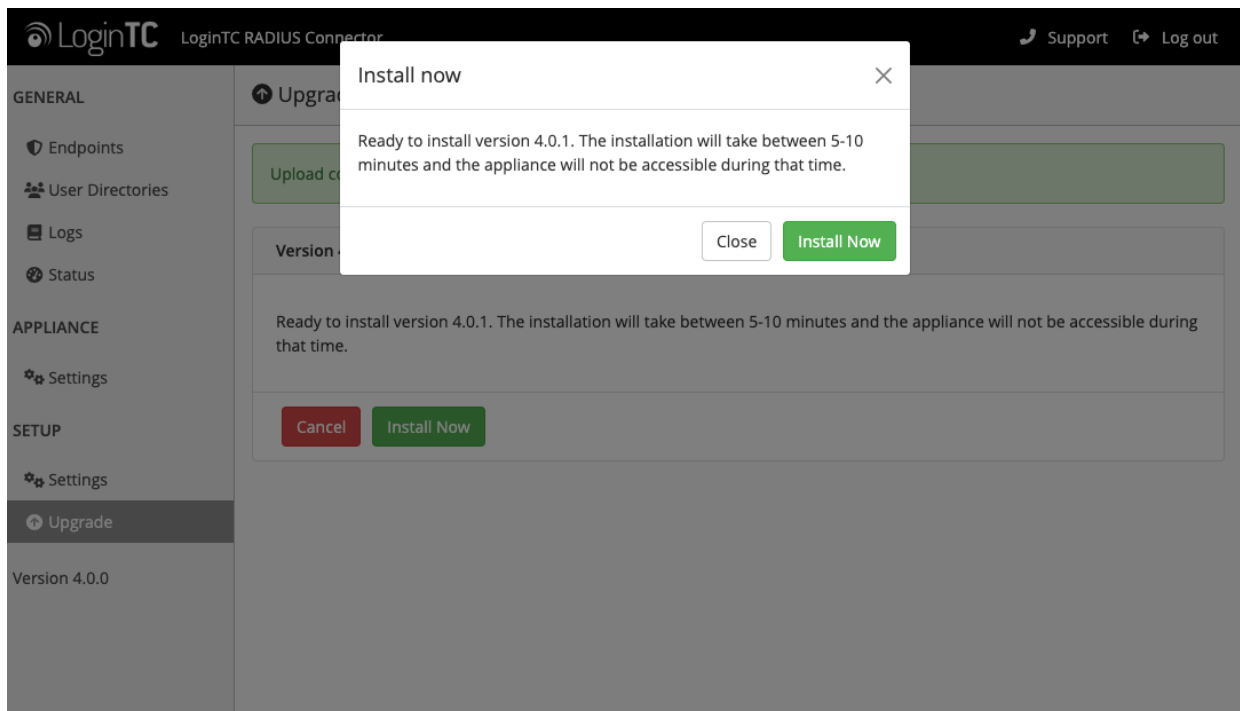
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



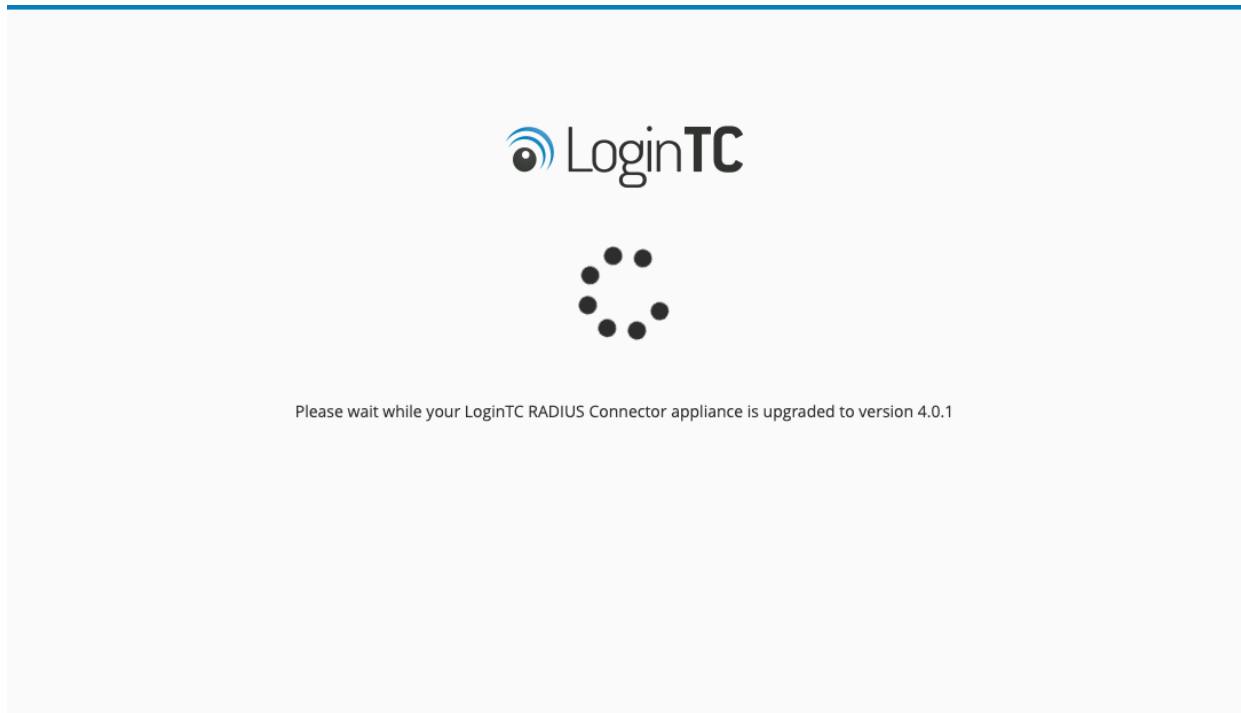
3. Click **Upload** and do not navigate away from the page:



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](#)