

RD Gateway Two-factor Authentication - LoginTC

logintc.com/docs/connectors/rd-gateway-radius

The [LoginTC RD Gateway with RADIUS Connector](#) protects access to your Microsoft Remote Desktop Gateway (RD Gateway) by adding a second factor LoginTC challenge to existing username and password authentication to your Remote Desktop resources.

This guide instructs you on how to configure your RD Gateway to use the LoginTC RADIUS Connector for two-factor authentication. If you would like to protect your RD Web Access then you may be interested in the: [LoginTC RD Web Access Connector](#).

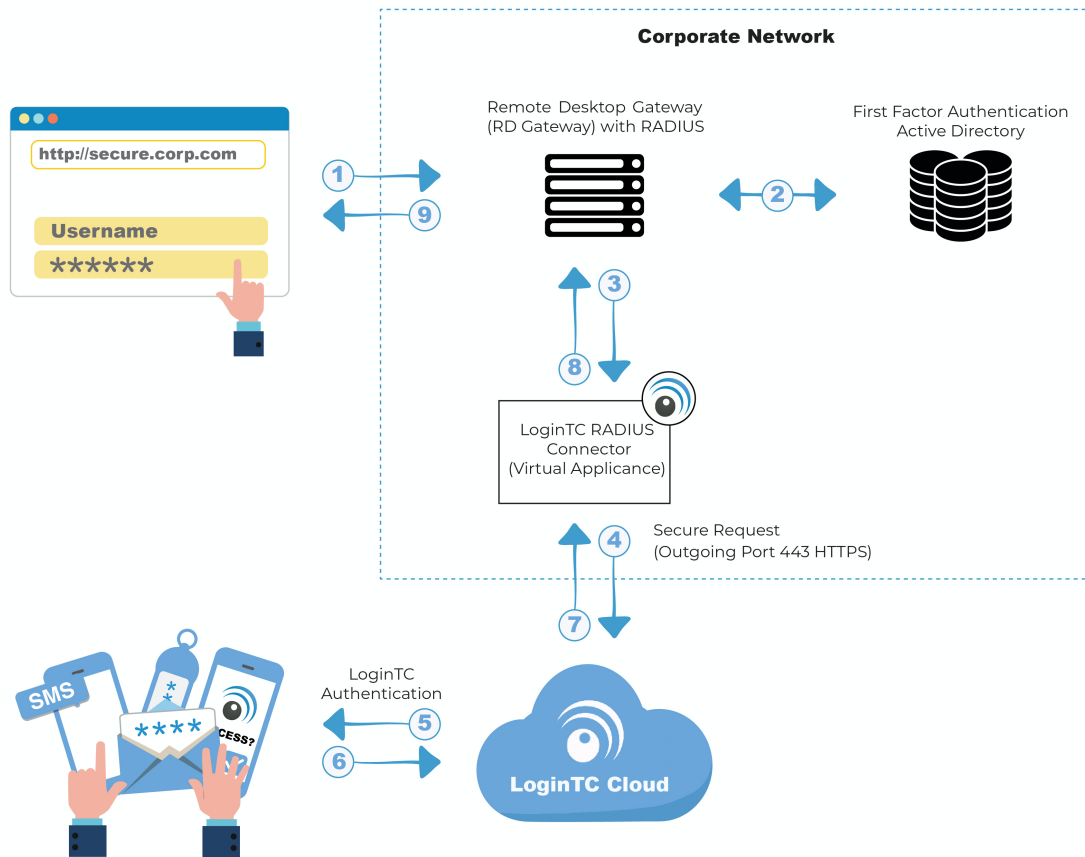
Note: Bypass Codes and OTPs not supported in this setup

As a result of how Microsoft implements using an external RADIUS authenticating server both bypass codes and OTPs are not supported for this setup. For bypass code and OTP support you may be interested in: [LoginTC RD Web Access Connector](#)

Video Instructions

Watch Video At: <https://youtu.be/FVw9iVFZ4J4>

Architecture



Authentication Flow

1. A user attempts access with their Remote Desktop client with username / password
2. The username / password is verified against an existing first factor directory (i.e. Active Directory)
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 Remote Desktop Gateway
9. User is granted access to Remote Desktop

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](#).

Normalize Usernames

Usernames in RD Gateway are typically in the form “CORP\john.doe”, while in the LoginTC Admin Panel it is generally more convenient to simply use “john.doe”.

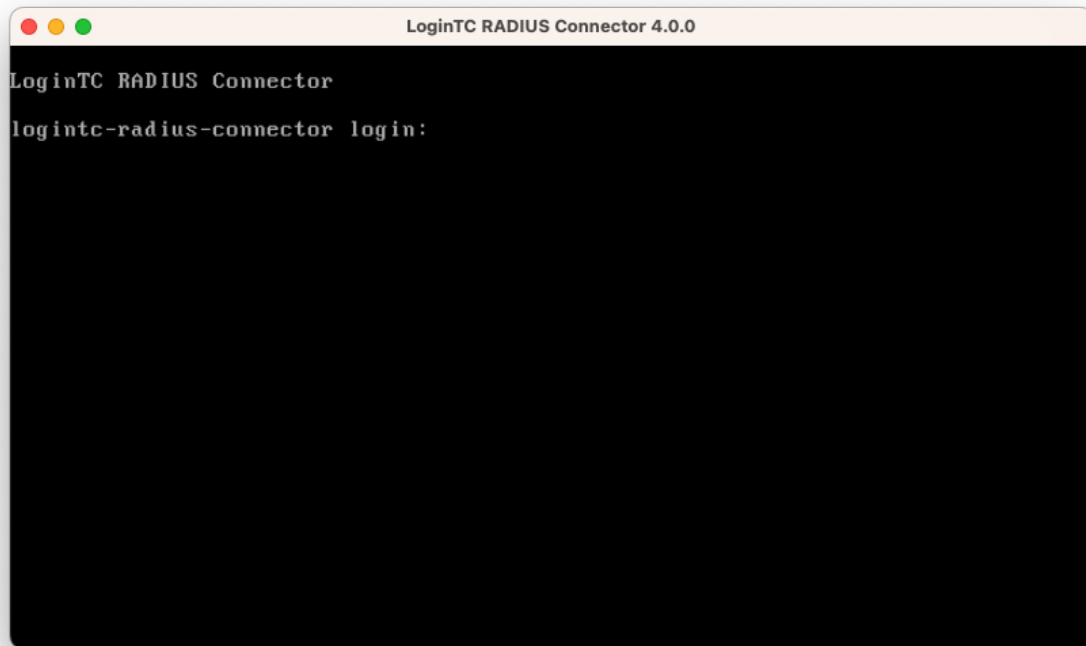
Configure **Normalize Usernames** from the Domain settings by navigating to **Domains > Your Domain > Settings**.

Select **Yes**, **Normalize Usernames** scroll down and click **Update**.

Installation

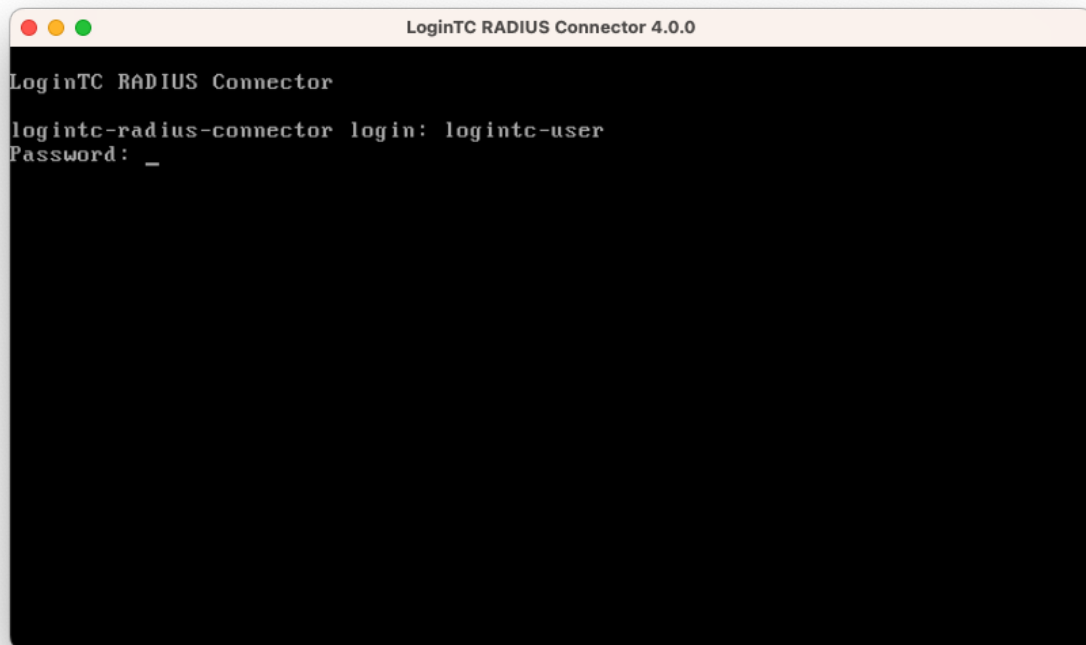
1. Import the virtual appliance your computer virtualization software
[Instructions for Hyper-V](#)
2. Ensure that LoginTC RADIUS CONNECTOR has a virtual network card
3. Start the virtual appliance

4. You will be with a console prompt:



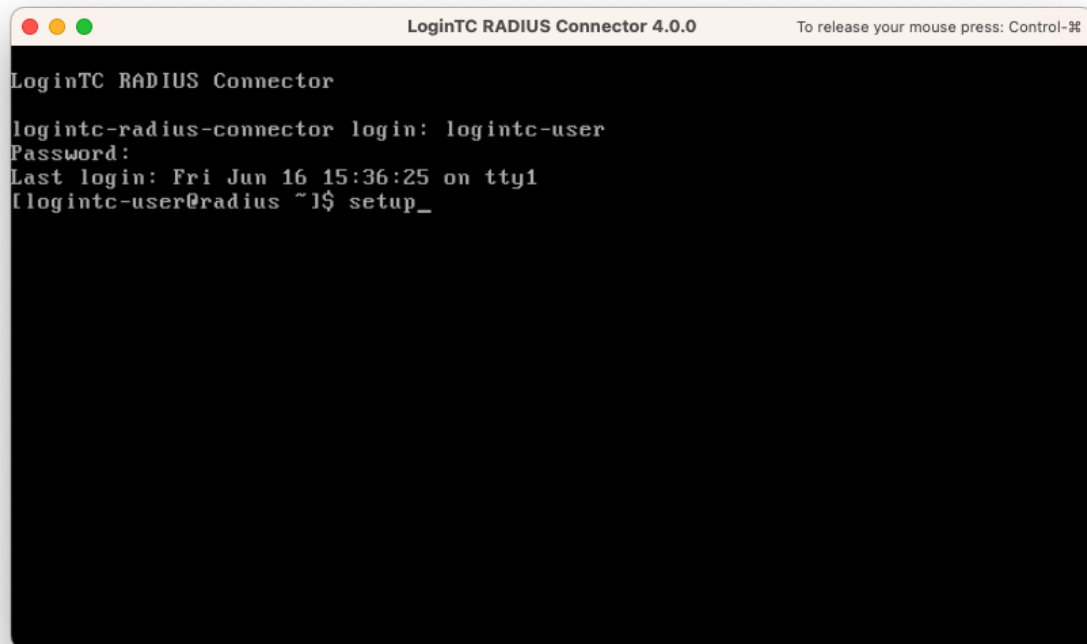
```
LoginTC RADIUS Connector 4.0.0
LoginTC RADIUS Connector
logintc-radius-connector login:
```

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



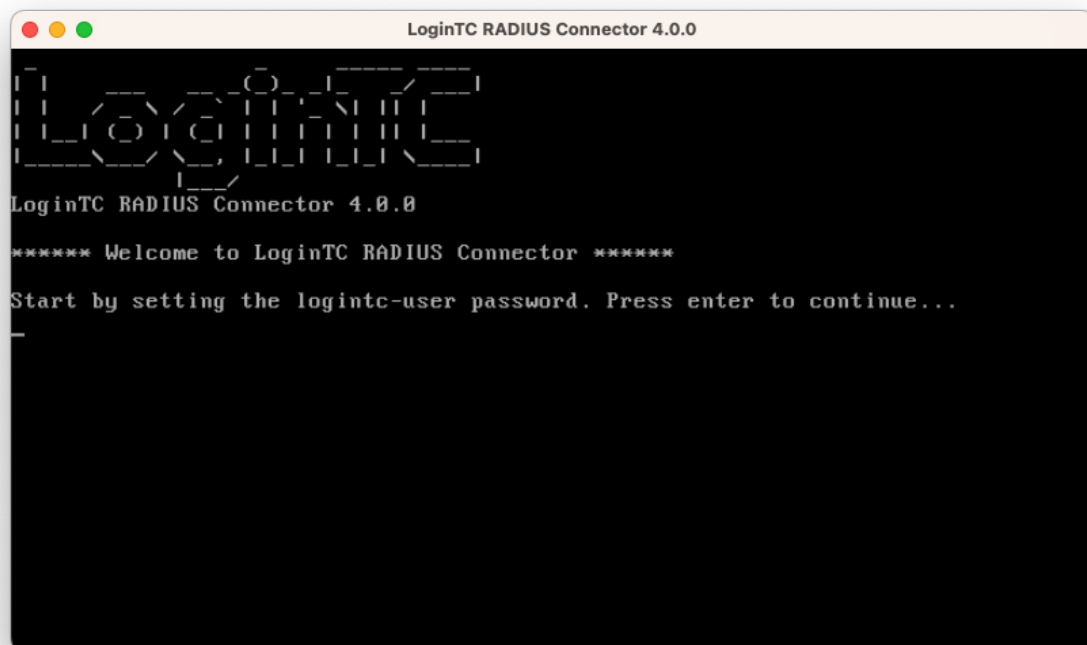
```
LoginTC RADIUS Connector 4.0.0
LoginTC RADIUS Connector
logintc-radius-connector login: logintc-user
Password: _
```

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



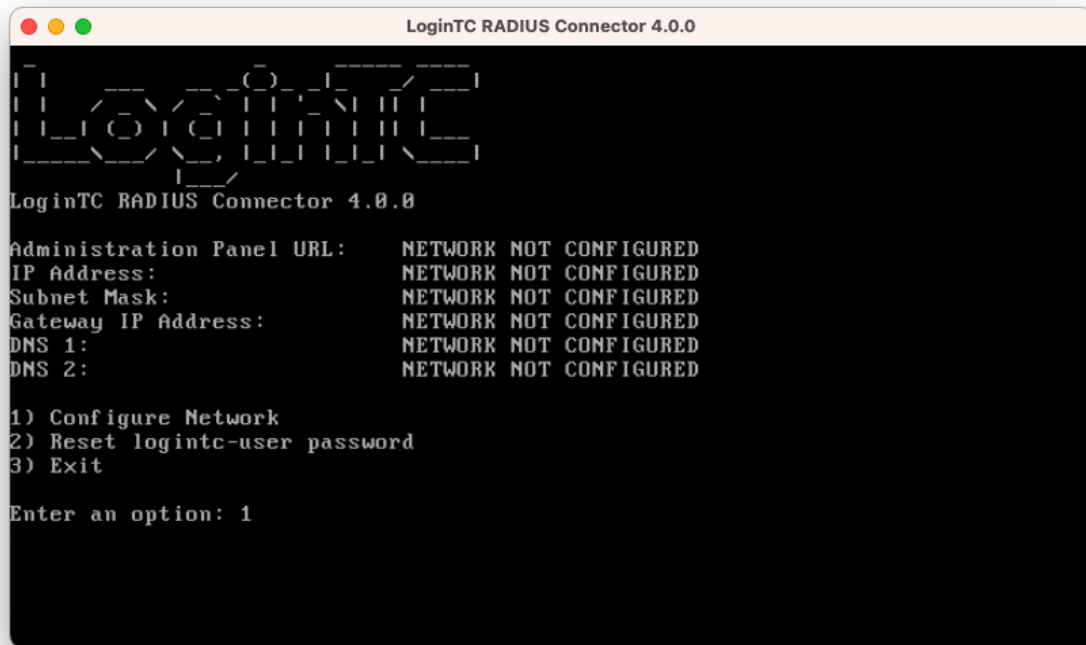
```
LoginTC RADIUS Connector 4.0.0 To release your mouse press: Control-⌘  
LoginTC RADIUS Connector  
logintc-radius-connector login: logintc-user  
Password:  
Last login: Fri Jun 16 15:36:25 on tty1  
[logintc-user@radius ~] $ setup_
```

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

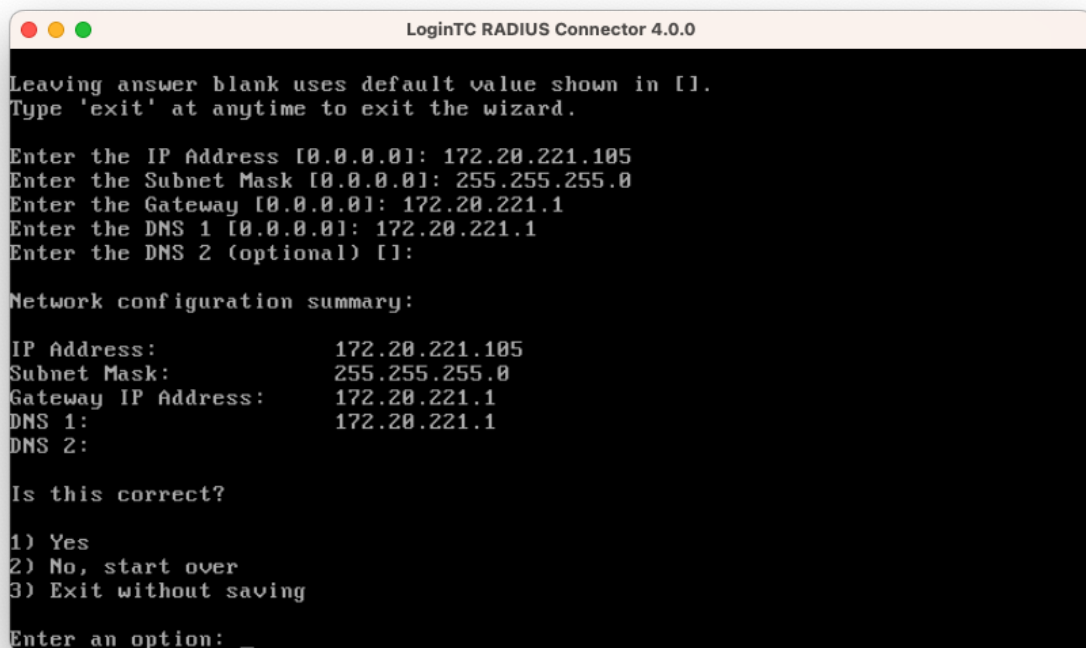


```
LoginTC RADIUS Connector 4.0.0  
┌───────────────────────────────────────────────────────────────────────────────────┐  
│                               LOGINTC RADIUS CONNECTOR                               │  
└───────────────────────────────────────────────────────────────────────────────────┘  
LoginTC RADIUS Connector 4.0.0  
***** Welcome to LoginTC RADIUS Connector *****  
Start by setting the logintc-user password. Press enter to continue...  
_
```

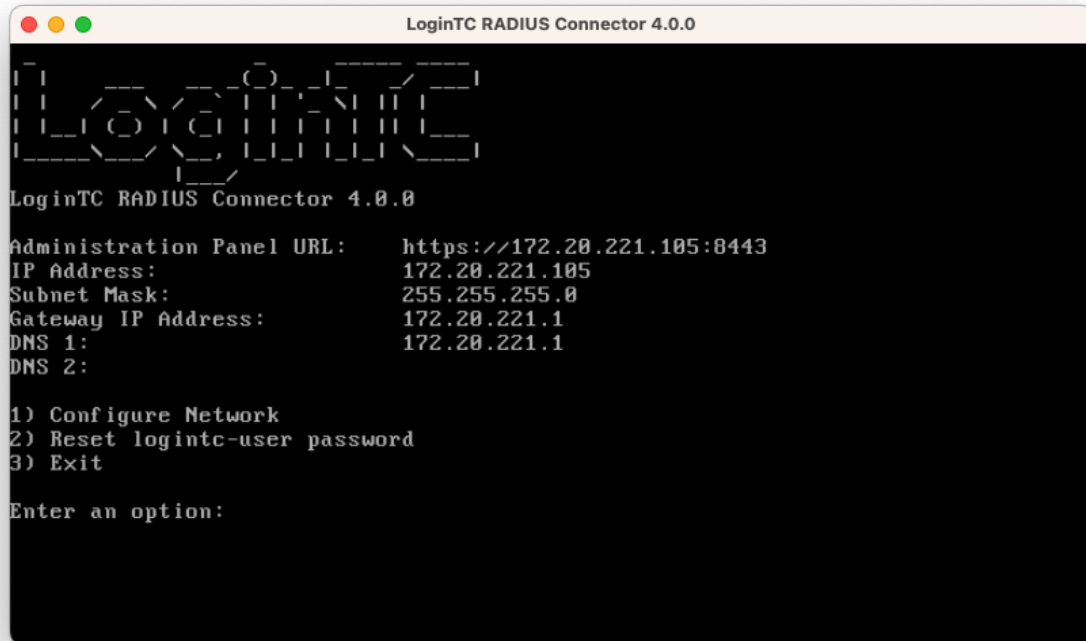
8. By default the appliance network is not configured. Manually configure the network by typing **1** and hit enter:



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>):

A screenshot of a terminal window titled "LoginTC RADIUS Connector 4.0.0". The terminal displays a logo for "LoginTC" in a stylized, dashed font. Below the logo, it shows the version "LoginTC RADIUS Connector 4.0.0". The network configuration is listed as follows: "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", and "DNS 2:". A menu with three options is shown: "1) Configure Network", "2) Reset logintc-user password", and "3) Exit". The prompt "Enter an option:" is at the bottom.

```

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

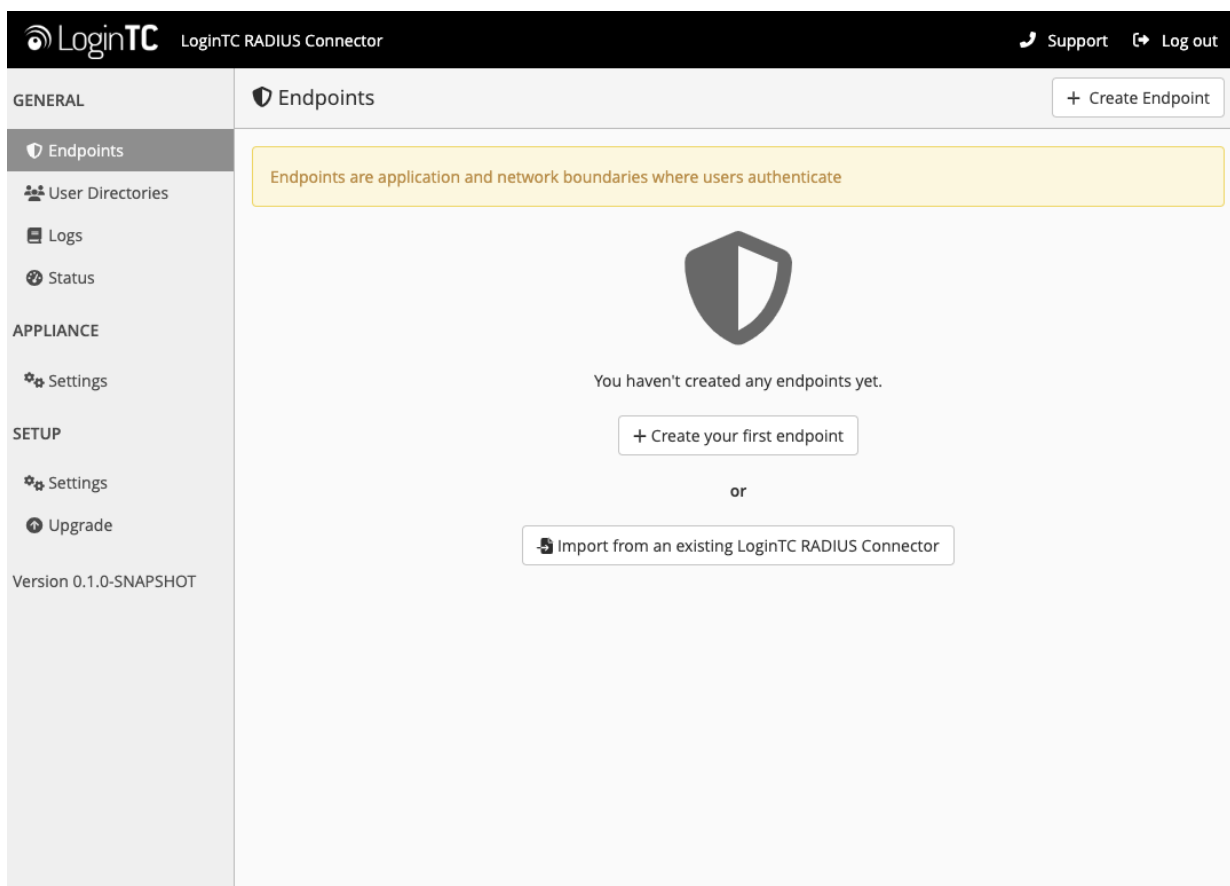
No, continue to the administration panel

[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 Remote Desktop Gateway 2FA

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

1. LoginTC Settings

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

2. User Directory

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

3. Challenge Strategy / Passthrough

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

4. Client Settings

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

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

First Endpoint

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

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

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



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:

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 RADIUS Connector Support Log out

GENERAL | **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

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.

Request Timeout

60

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:

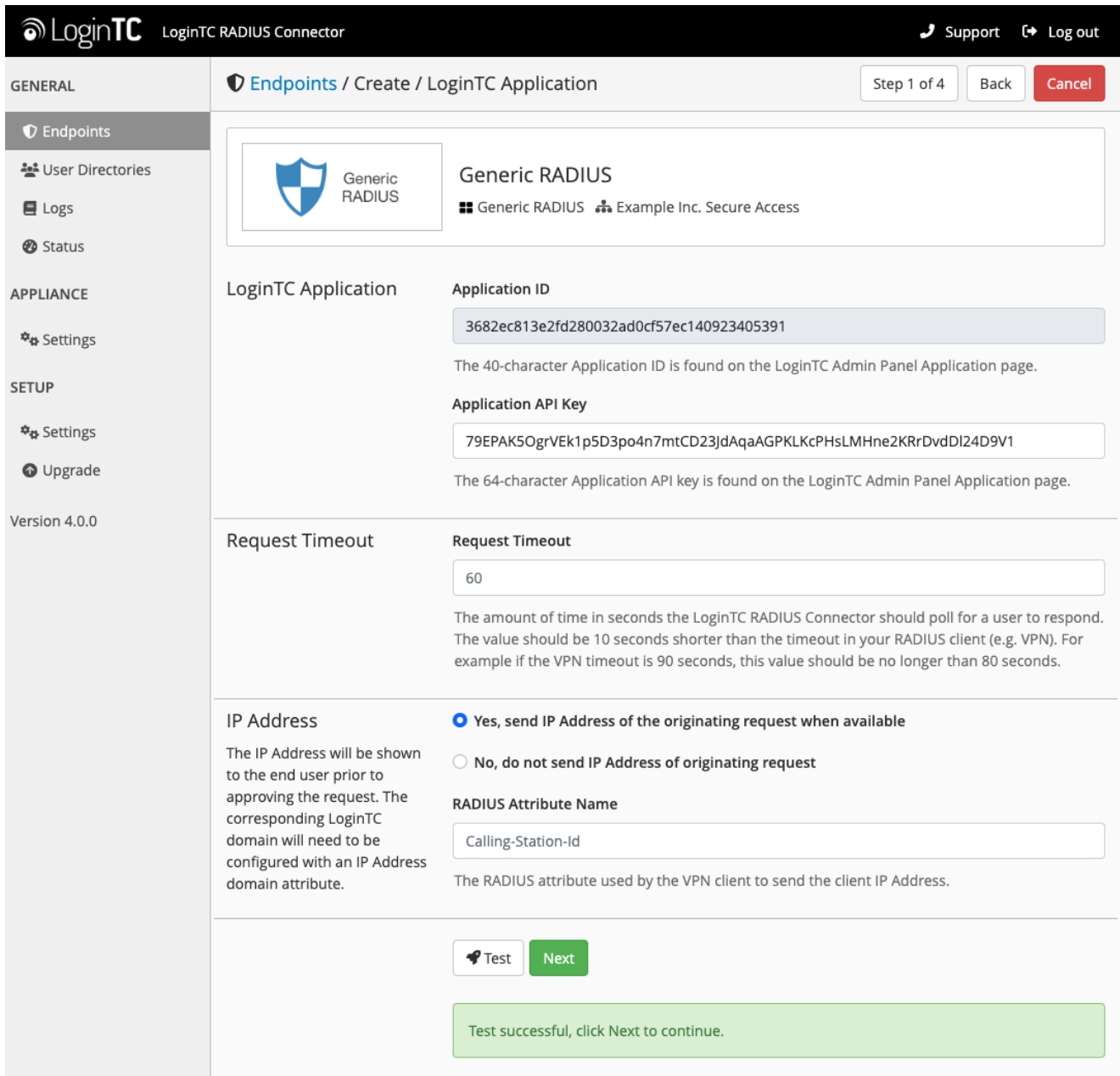
| Property | Explanation |
|---------------------|--|
| Application ID | The 40-character Application ID, retrieve Application ID |
| Application API Key | The 64-character Application API Key, retrieve Application API Key |
| Request Timeout | Number of seconds that the RADIUS connector will wait for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

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:

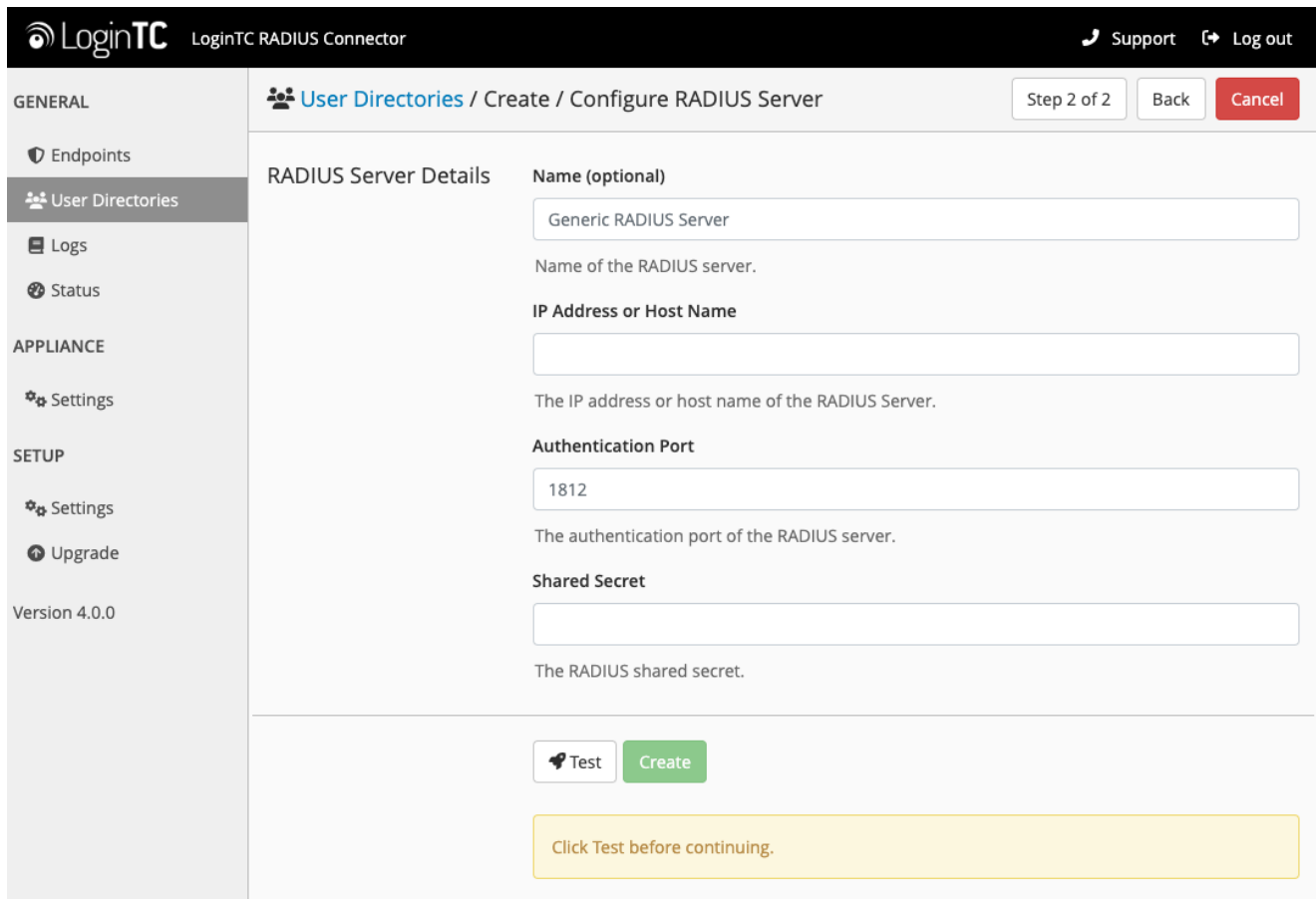
| Property | Explanation | Examples |
|-----------------|---|----------------------------------|
| host | Host or IP address of the LDAP server | ldap.example.com or 192.168.1.42 |
| port (optional) | Port if LDAP server uses non-standard (i.e., 389/636) | 4000 |
| bind_dn | DN of a user with read access 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> |
| 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 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 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'. A yellow instruction box at the top reads: 'Select which users should be challenges with LoginTC and which should bypass LoginTC'. Three options are presented in a list:

- Challenge All Users**: All users will be challenged with LoginTC. (This option is selected, indicated by a checkmark icon.)
- Challenge Users Based on Static Username List**: Only users in a static username list will be challenged with LoginTC.
- Challenge Users Based on Group Membership**: Leverage Active Directory and LDAP Group Membership to determine which users are challenges with LoginTC and which users bypass LoginTC.

The left sidebar contains navigation links for 'GENERAL' (Endpoints, User Directories, Logs, Status) and 'APPLIANCE' (Settings). The 'SETUP' section includes 'Settings' and 'Upgrade' links. The version number 'Version 4.0.0' is displayed at the bottom of the sidebar.

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.

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)
Generic RADIUS
Name for the endpoint.

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

Shared Secret
The RADIUS shared secret.

Authentication Mode Direct Iframe Challenge Challenge Interactive
How the LoginTC authentication is performed Send authentication request directly and automatically.

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

Testing

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

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

Example Inc. Business Docs Support administrator@example.com

Domains / Example Inc. Secure Access + Create Member Members Settings

Members

Example Inc. Secure Access has 88 member(s)

+ Create Member View Members

Attributes

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

+ Create Domain Attribute

Latest Actions

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

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

Example Inc. Business Docs Support administrator@example.com

Domains / Example Inc. Secure Access / Members + Create Member Settings

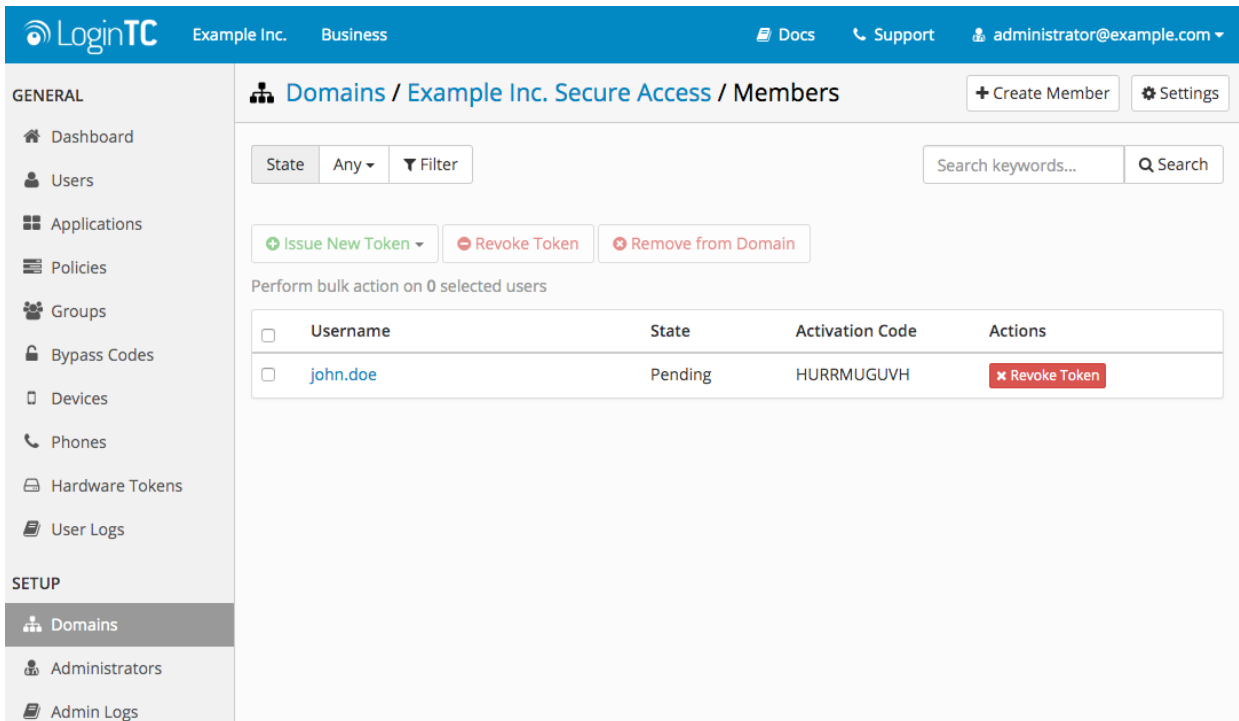
State Any Filter Search keywords... Search

+ Issue New Token - Revoke Token - Remove from Domain

Perform bulk action on 0 selected users

| <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:

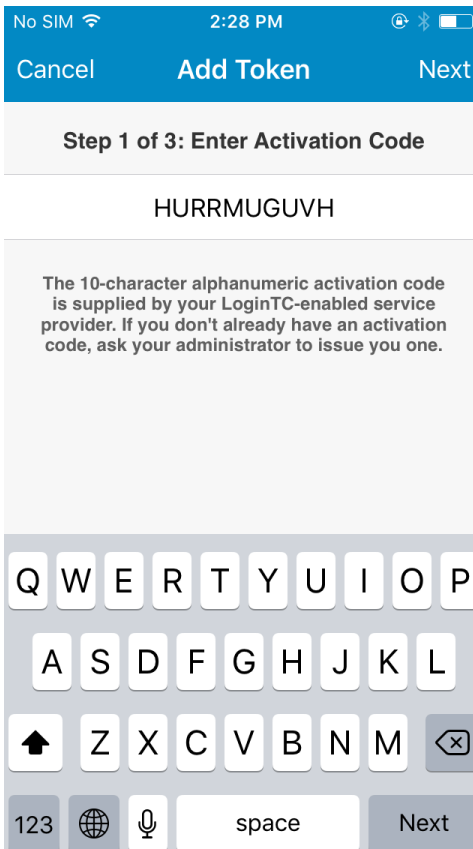


The screenshot shows the LoginTC web interface for 'Example Inc. Business'. The left sidebar contains navigation options under 'GENERAL' (Dashboard, Users, Applications, Policies, Groups, Bypass Codes, Devices, Phones, Hardware Tokens, User Logs) and 'SETUP' (Domains, Administrators, Admin Logs). The main content area is titled 'Domains / Example Inc. Secure Access / Members' and includes a search bar and buttons for 'Issue New Token', 'Revoke Token', and 'Remove from Domain'. A table lists users with columns for Username, State, Activation Code, and Actions. The user 'john.doe' is shown with a 'Pending' state and an activation code 'HURRMUGUVH', with a 'Revoke Token' button next to it.

| Username | State | Activation Code | Actions |
|----------|---------|-----------------|--------------|
| john.doe | Pending | HURRMUGUVH | Revoke Token |

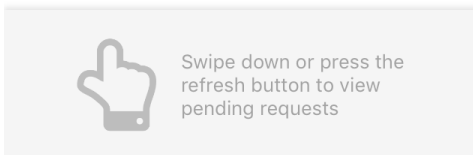
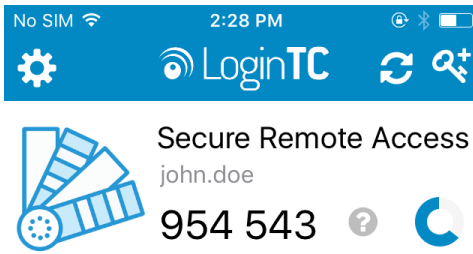
7. Open the LoginTC mobile app.

8. Enter the 10-character alphanumeric activation code:



The screenshot shows the LoginTC mobile app interface. At the top, there is a status bar with 'No SIM', signal strength, time '2:28 PM', and battery level. Below the status bar is a blue header with 'Cancel', 'Add Token', and 'Next' buttons. The main content area is titled 'Step 1 of 3: Enter Activation Code' and displays the activation code 'HURRMUGUVH'. Below the code, there is a text box explaining: '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.' At the bottom, there is a keyboard with a 'Next' button.

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 

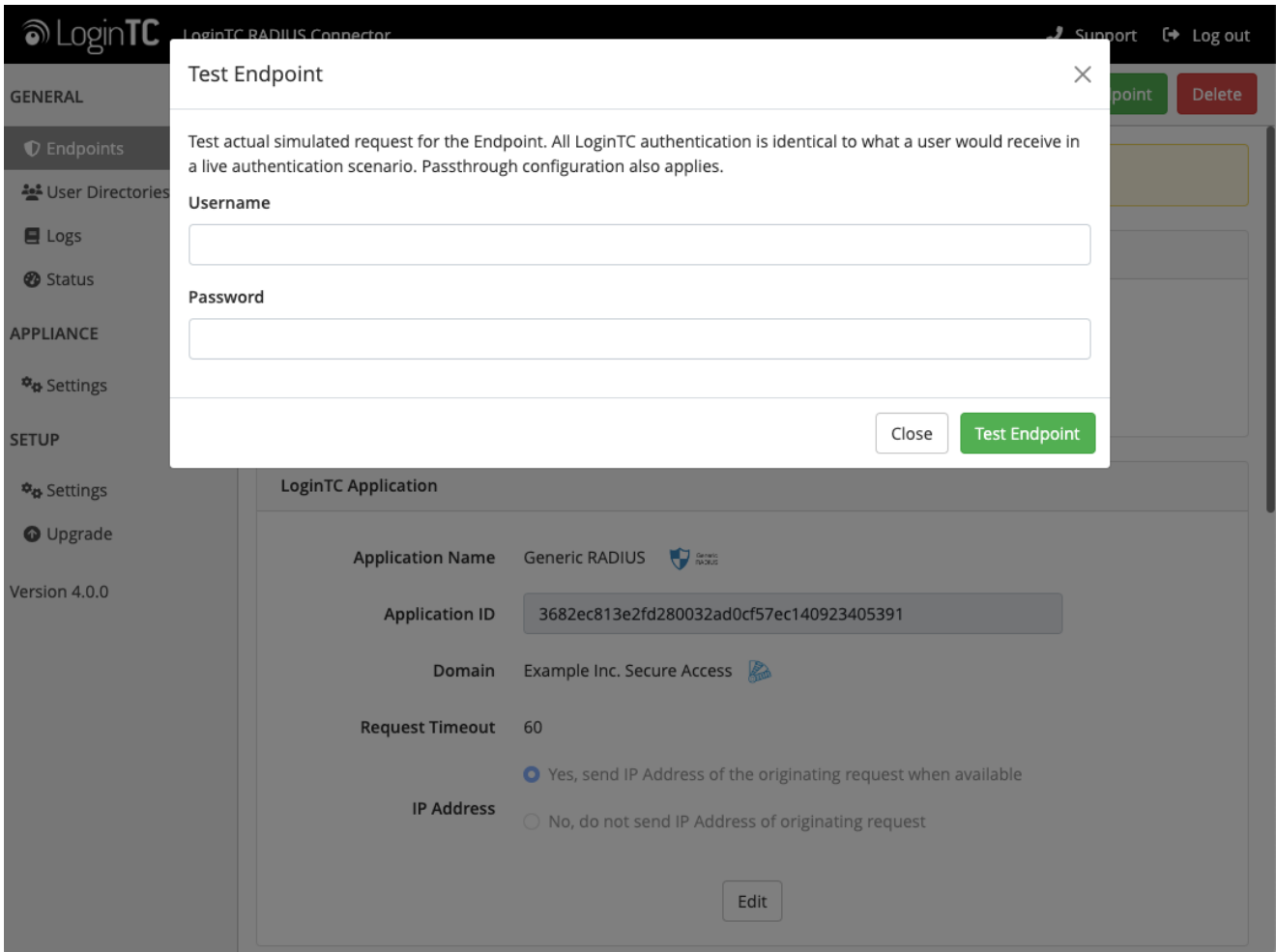
Request Timeout 60

Yes, send IP Address of the originating request when available

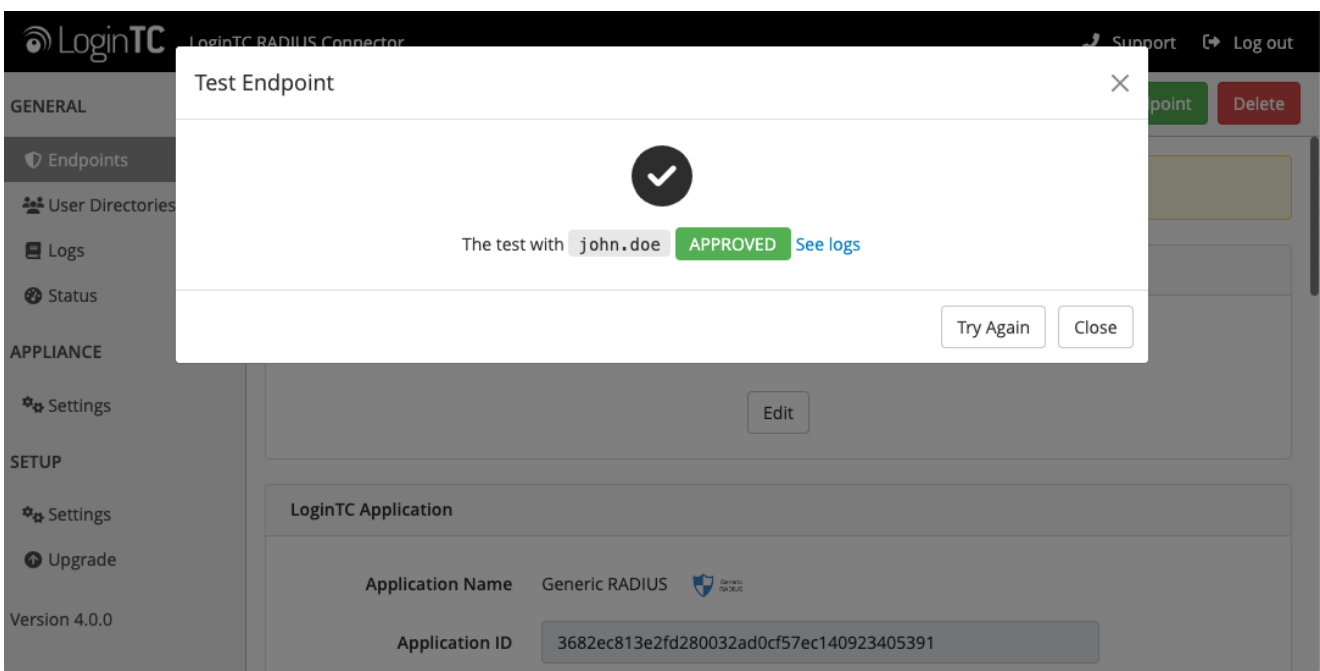
IP Address No, do not send IP Address of originating request

Edit

Click Test Configuration:

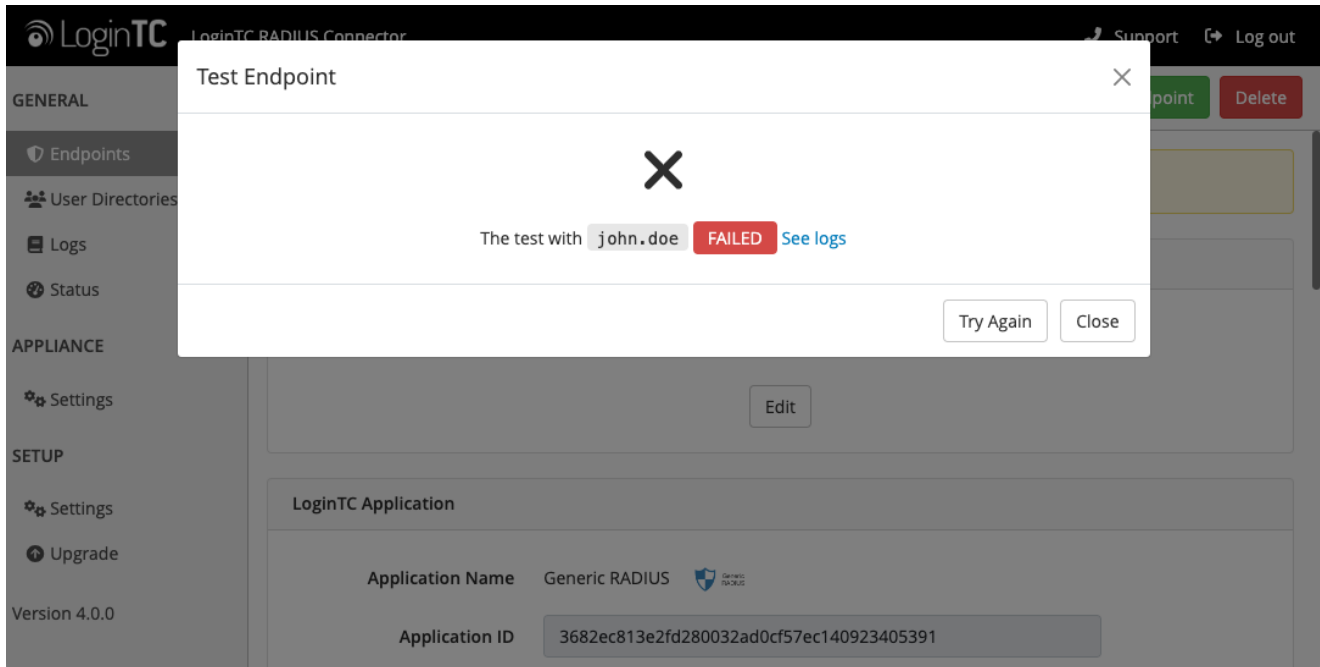


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

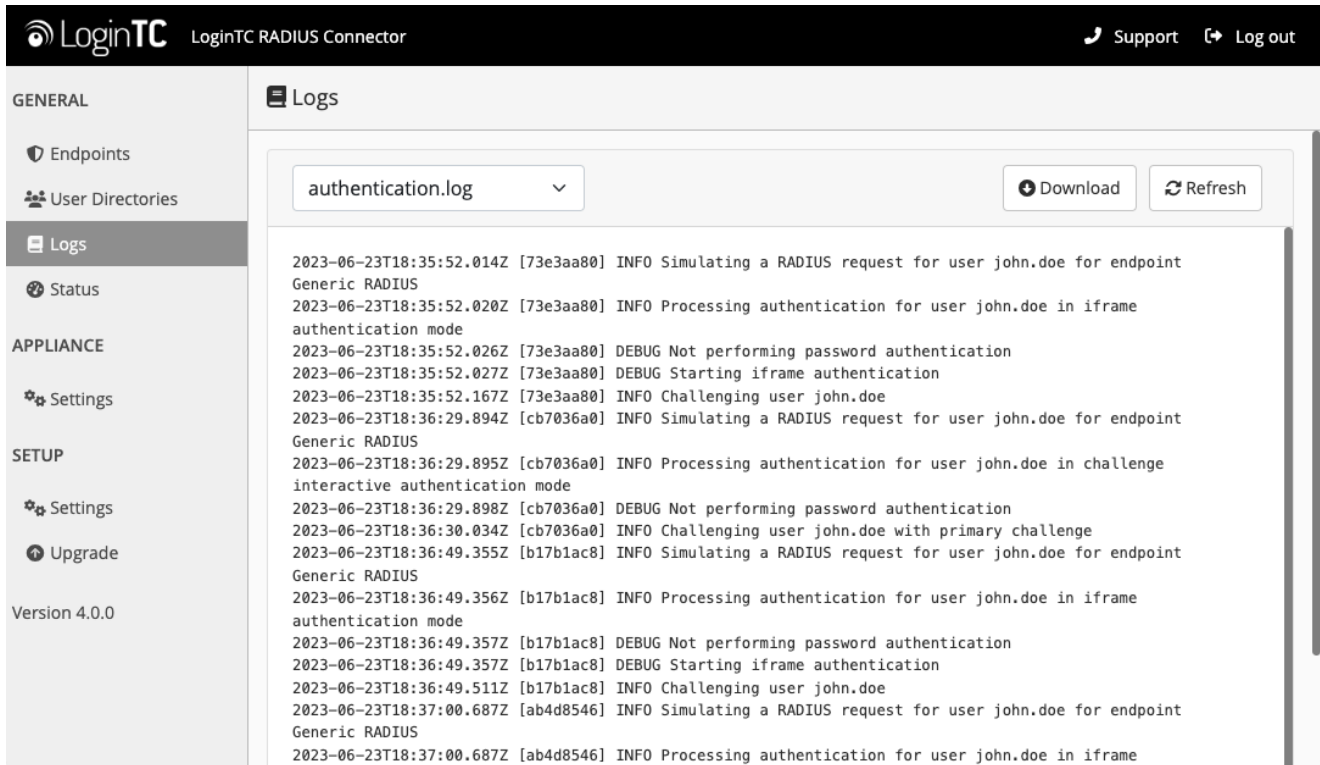


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



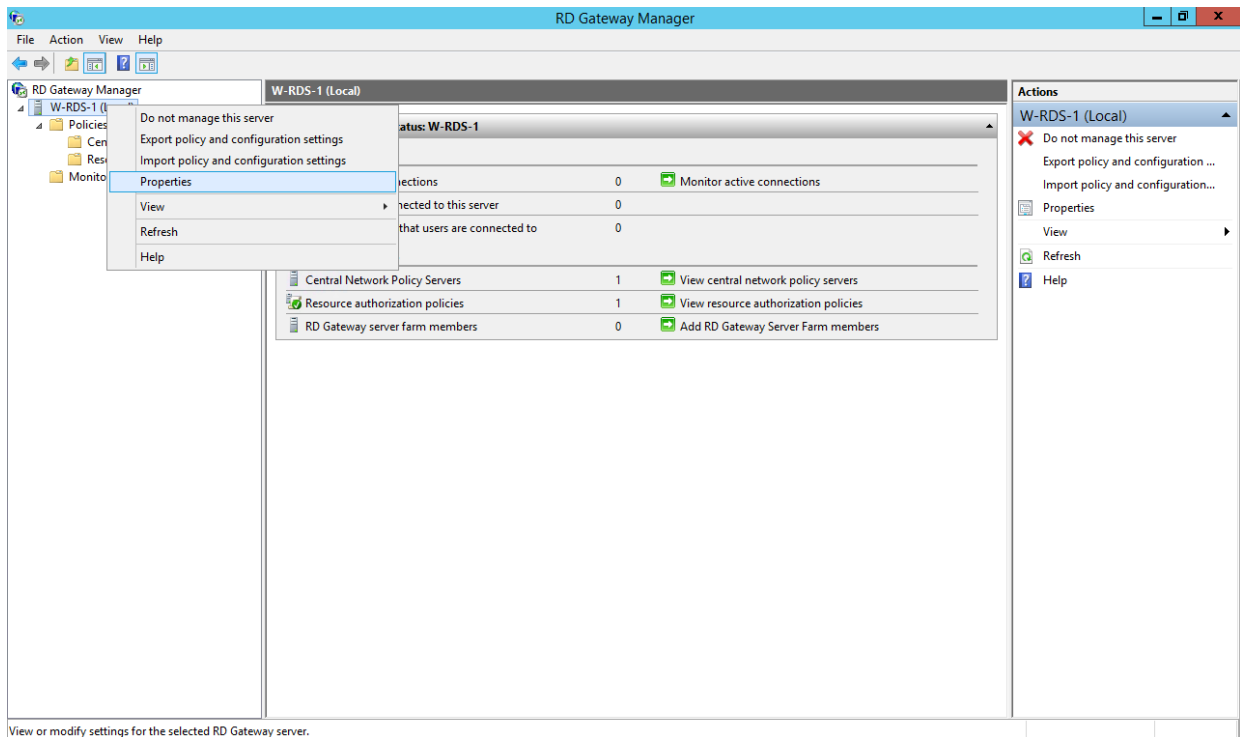
In this case, click **See logs** (or click the **Logs** section):



RD Gateway Configuration

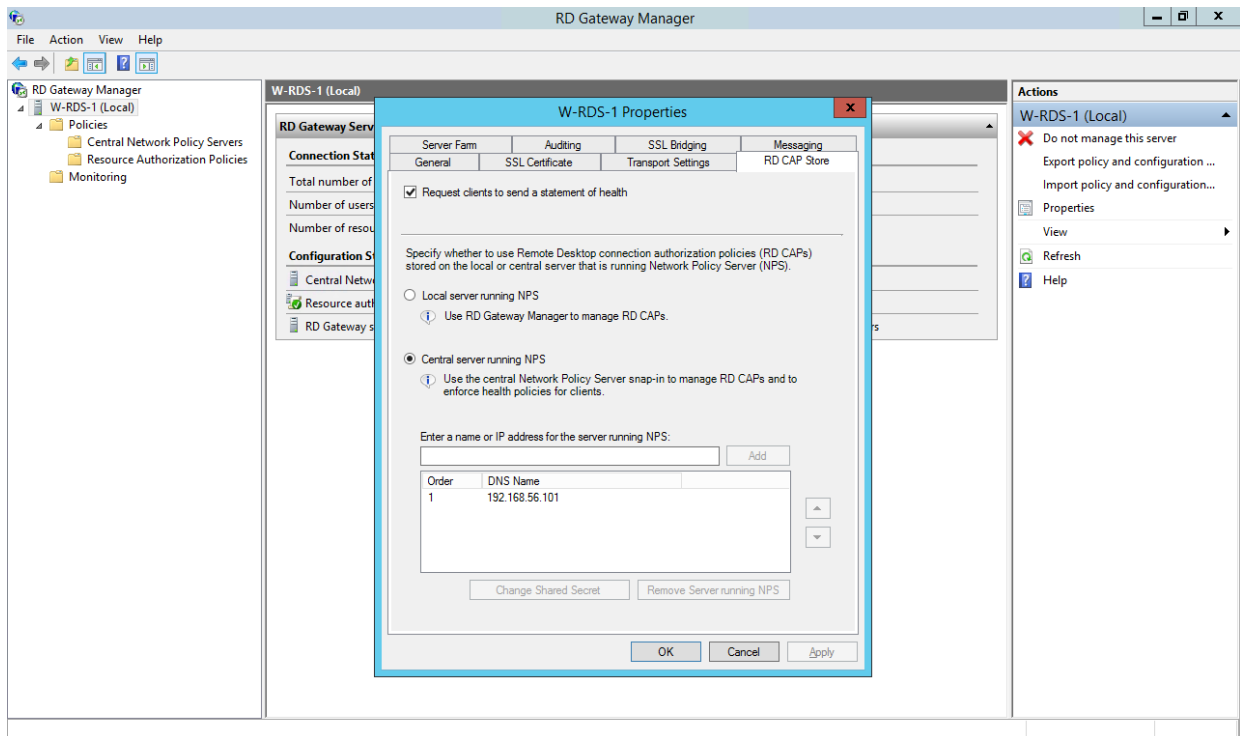
Once you have configured the LoginTC RADIUS Connector you will be able to configure your RD Gateway to use the LoginTC RADIUS Connector for second-factor authentication.

1. Open the **RD Gateway Manager** from your Start Menu
2. Right click on your RD server in the left sidebar and click on Properties



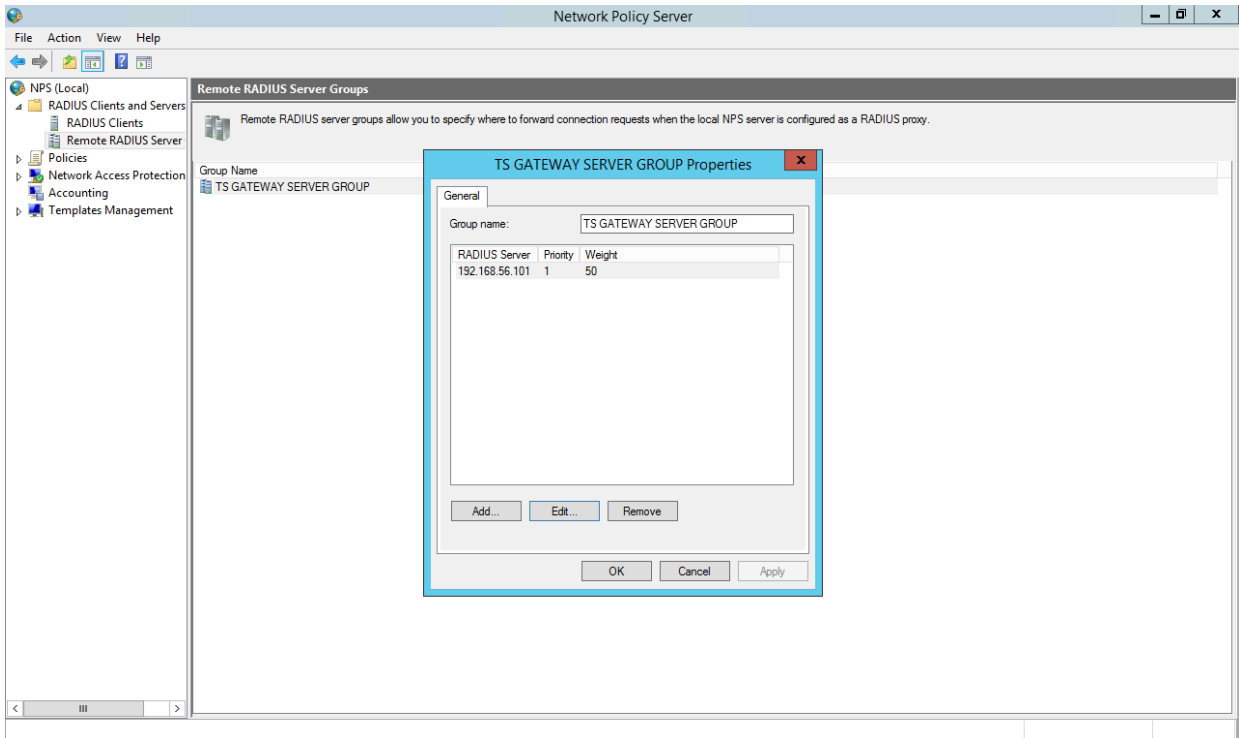
3. Select the **RD CAP Store** tab
4. Select **Central server running NPS** radio button
5. Enter the IP address of your LoginTC RADIUS Connector and press **Add** button

6. Enter the shared secret that you configured on the LoginTC RADIUS Connector and press **OK**



7. Press the **Apply** button
8. Press the **OK** button
9. Open the **Network Policy Server** manager
10. Expand **RADIUS Clients and Servers** in the left sidebar
11. Select **Remote RADIUS Server**

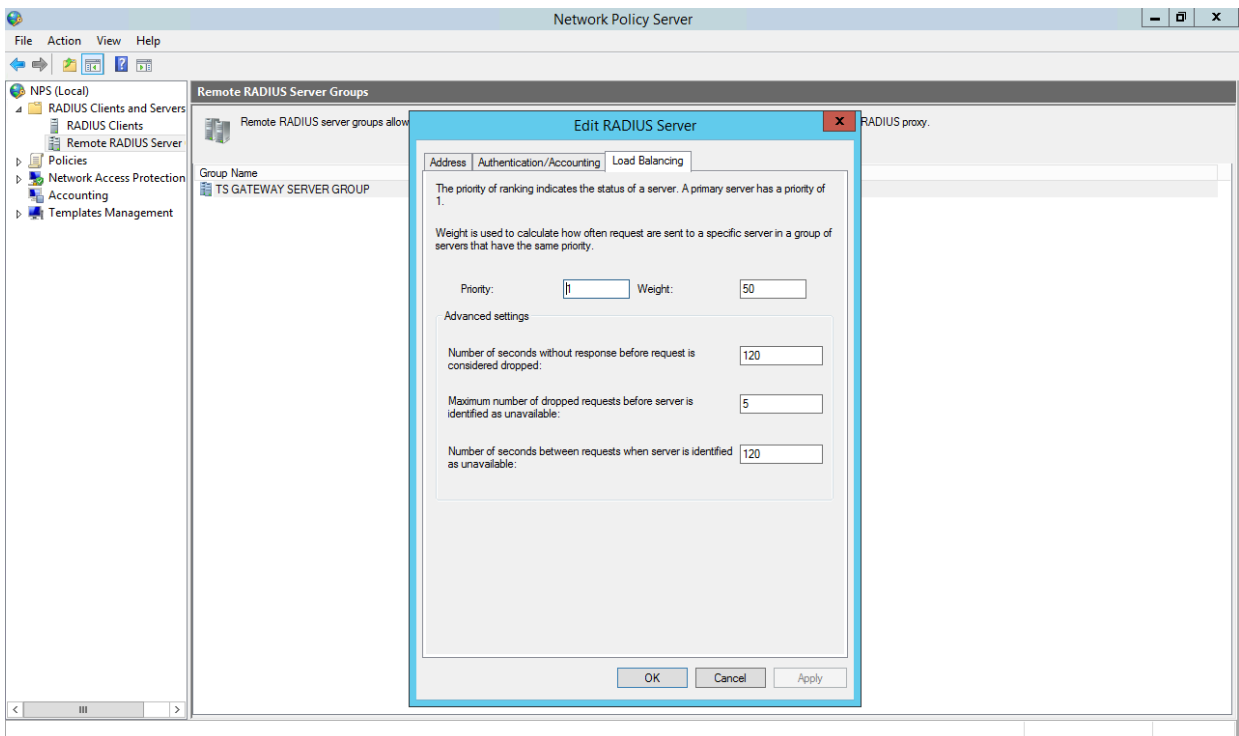
12. Right click on **TS GATEWAY SERVER GROUP** and click on **Properties**



13. Select your RADIUS server and press **Edit...**

14. Select the **Load Balancing** tab

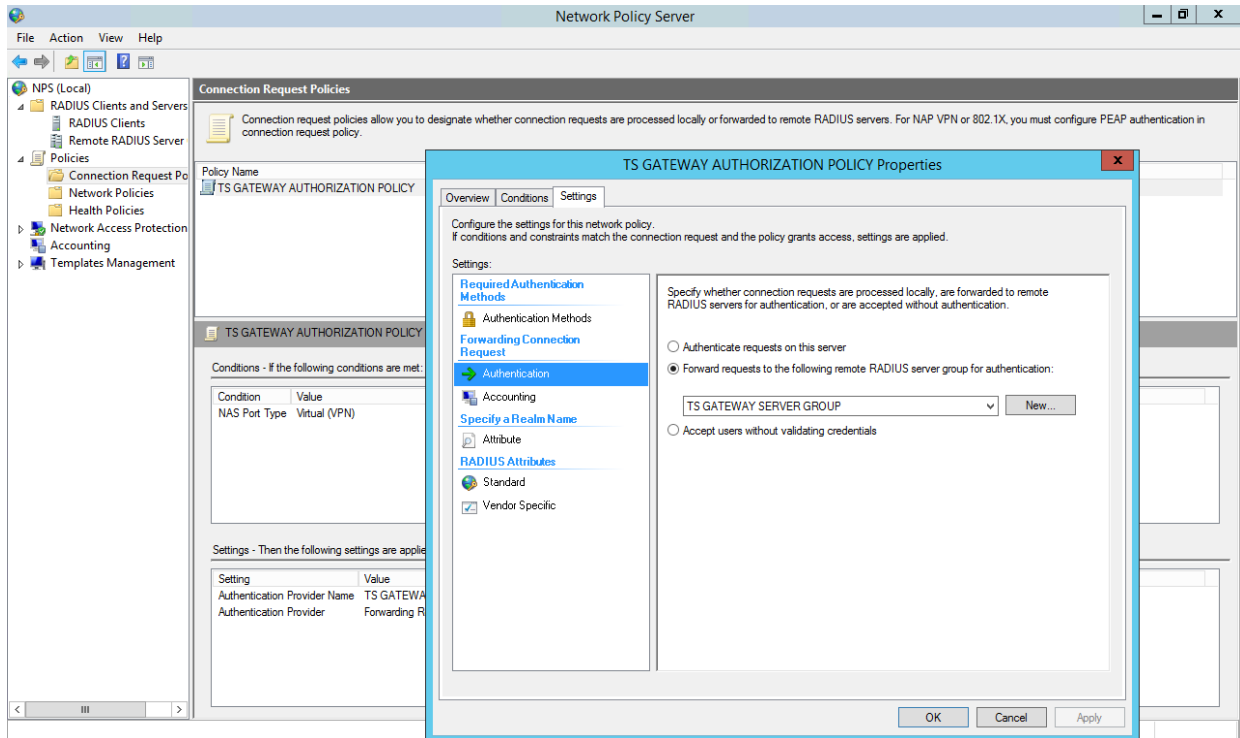
15. Set the timeout settings to 120 seconds



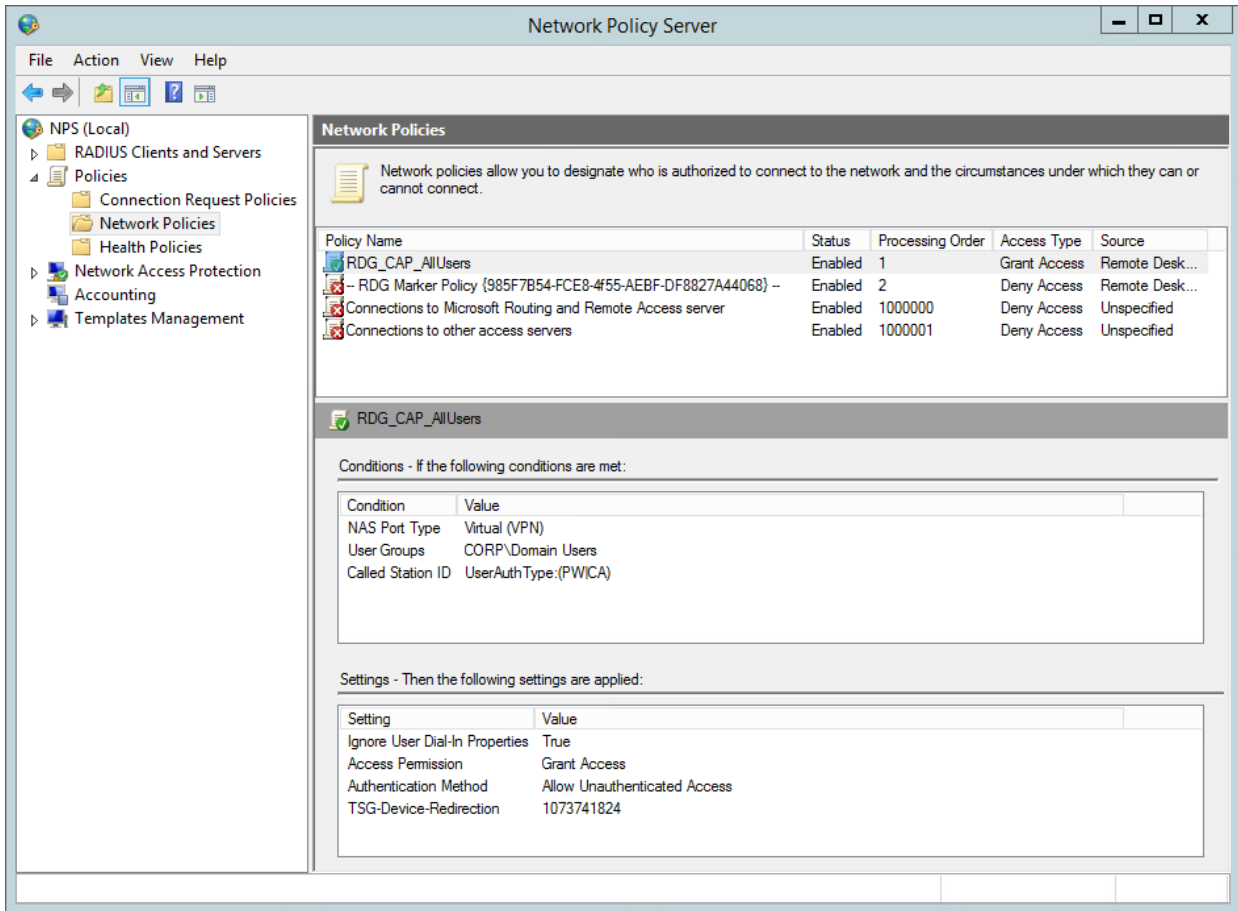
16. Press the **Apply** button

17. Press the **OK** button to close the dialog

18. Expand **Policies** in the left sidebar
19. Click on **Connection Request Policies**
20. Right click on **TS GATEWAY AUTHORIZATION POLICY** and click on **Properties**
21. Click on **Settings** tab
22. Select **Authentication** and ensure that it's set to **Forward requests** to the remote RADIUS server

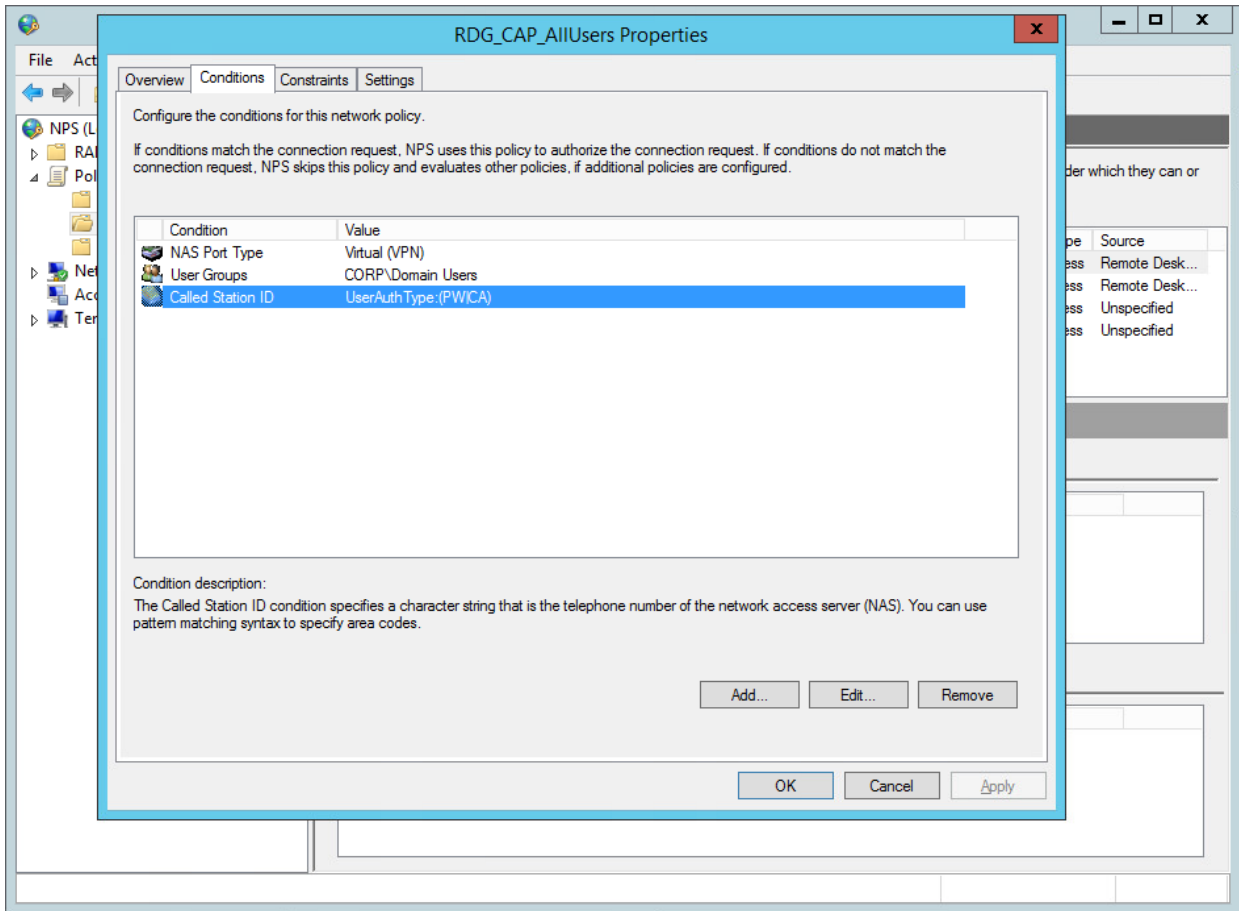


23. Click on **Policies** → **Network Policies**



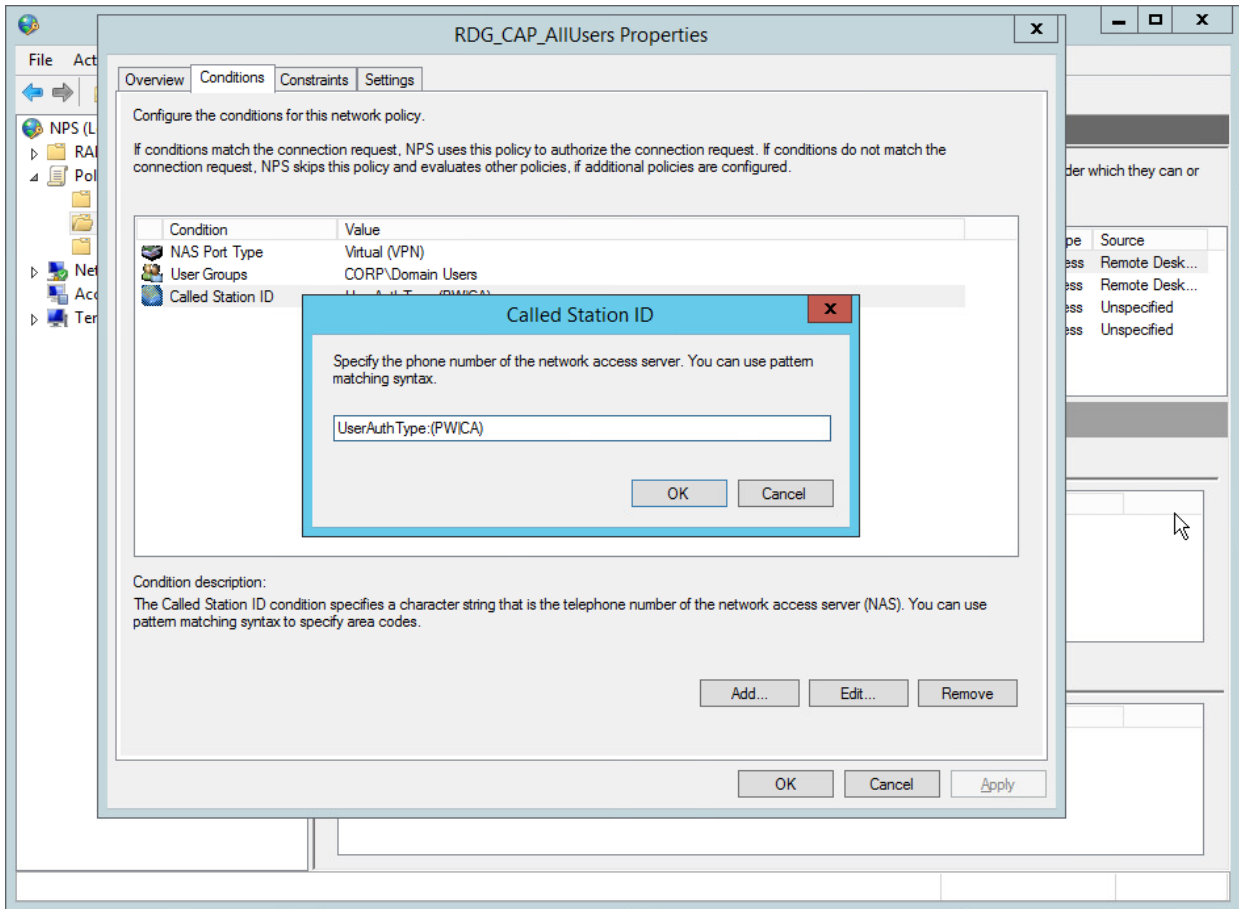
24. Double click on your RDG CAP policy

25. Click on the **Conditions** tab



26. Select the **Called Station ID** attribute and press the **Edit...** button

27. Set the value to **UserAuthType:(PW|CA)**



28. Press the **OK** button

29. Press the **Apply** button

You may now test your RD Gateway.

User Management


Create users in LoginTC corresponding to your AD/LDAP users and provision them tokens. 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 to LoginTC Admin is performed using [User Sync Tool](#).

For more details about user management and provisioning, visit the [User Management](#) guide.

Logging

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

 LoginTC RADIUS Connector

 Support
  Log out

GENERAL

- Endpoints
- User Directories
- Logs
- Status

APPLIANCE

- Settings

SETUP

- Settings
- Upgrade

Version 4.0.0

Logs


```



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 LoginTC RADIUS Connector appliance **web interface** URL and click **Status**:

 LoginTC RADIUS Connector

 Support
  Log out

GENERAL

- Endpoints
- User Directories
- Logs
- Status

APPLIANCE

- Settings

SETUP

- Settings
- Upgrade

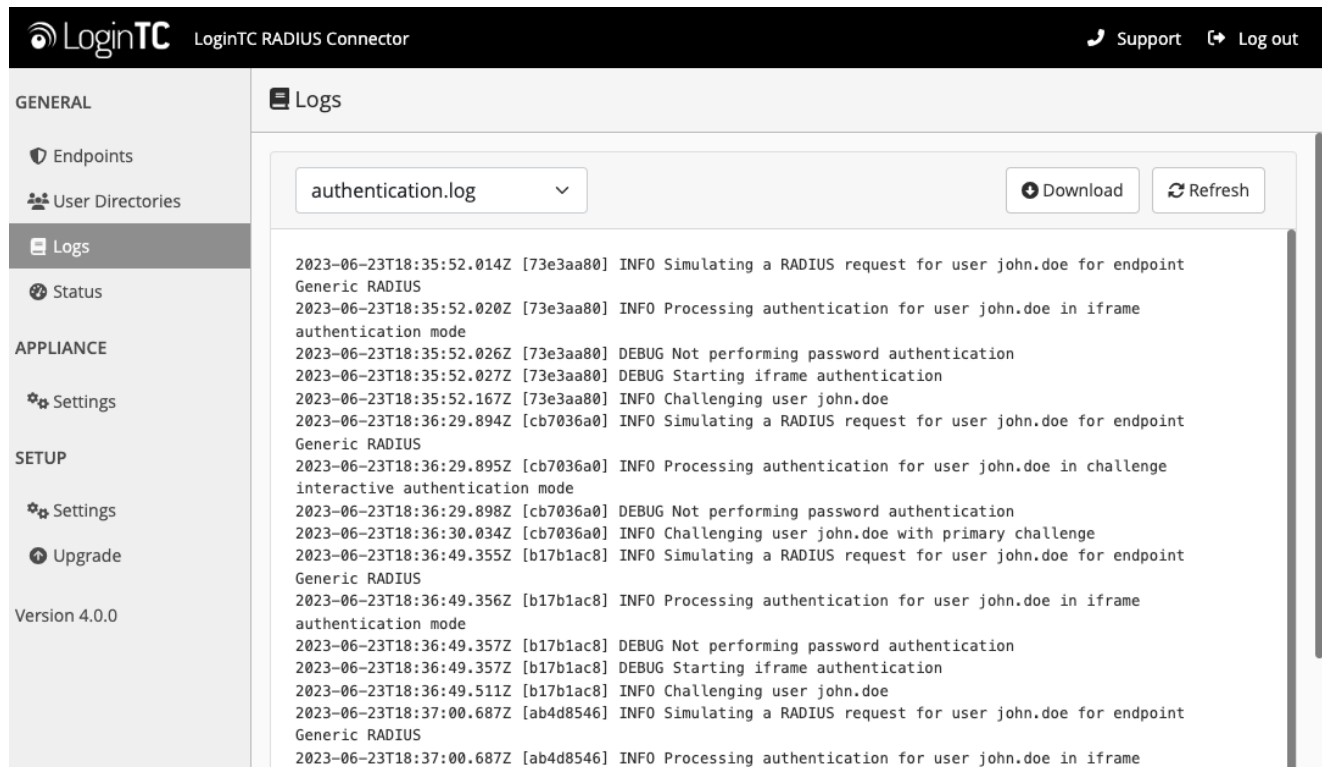
Version 4.0.0

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**:



The screenshot shows the LoginTC RADIUS Connector 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 'Logs' selected, and other sections like 'APPLIANCE' and 'SETUP'. The main content area is titled 'Logs' and shows a dropdown menu with 'authentication.log' selected. Below the dropdown are 'Download' and 'Refresh' buttons. The log content consists of multiple lines of text, each starting with a timestamp and an IP address, followed by a log level (INFO or DEBUG) and a description of the event, such as 'Simulating a RADIUS request for user john.doe' or 'Processing authentication for user john.doe'.

You may also find valuable information in the Microsoft **Event Viewer** under **Custom Views** → **ServerRoles** → **Network Policy and Access Services**

Email Support

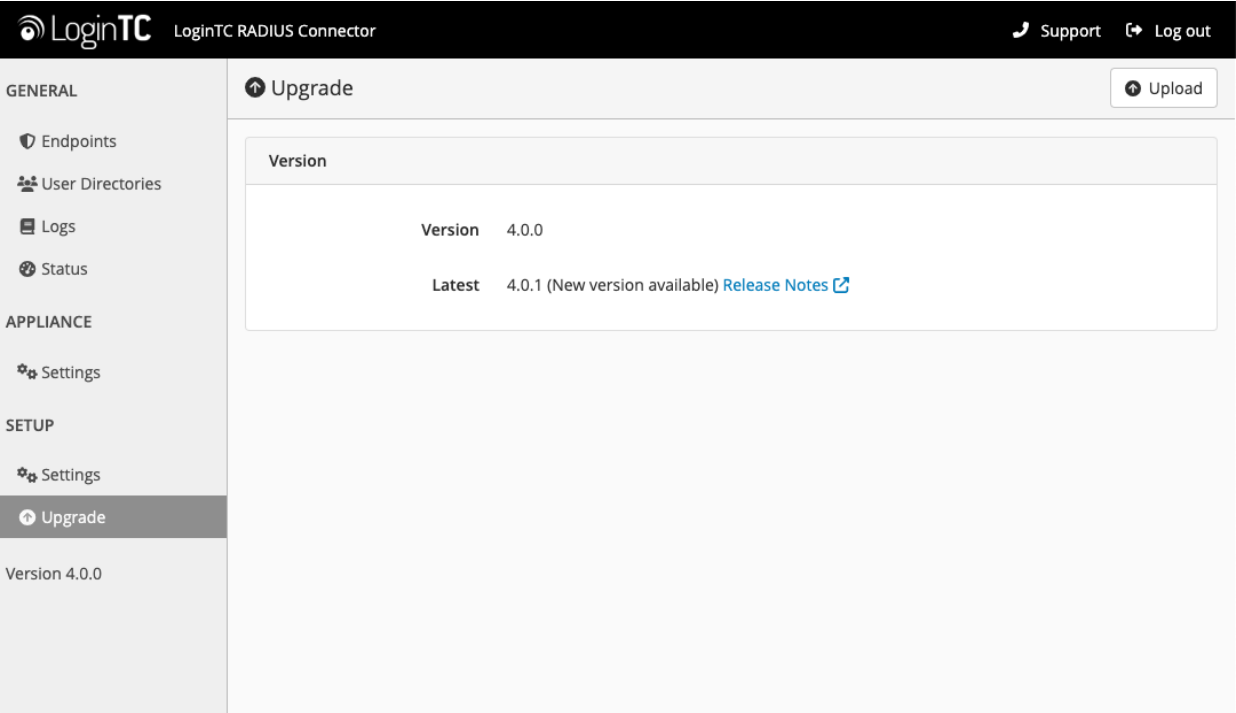
For any additional help please email support@cyphercor.com. Expect a speedy reply.

Upgrading

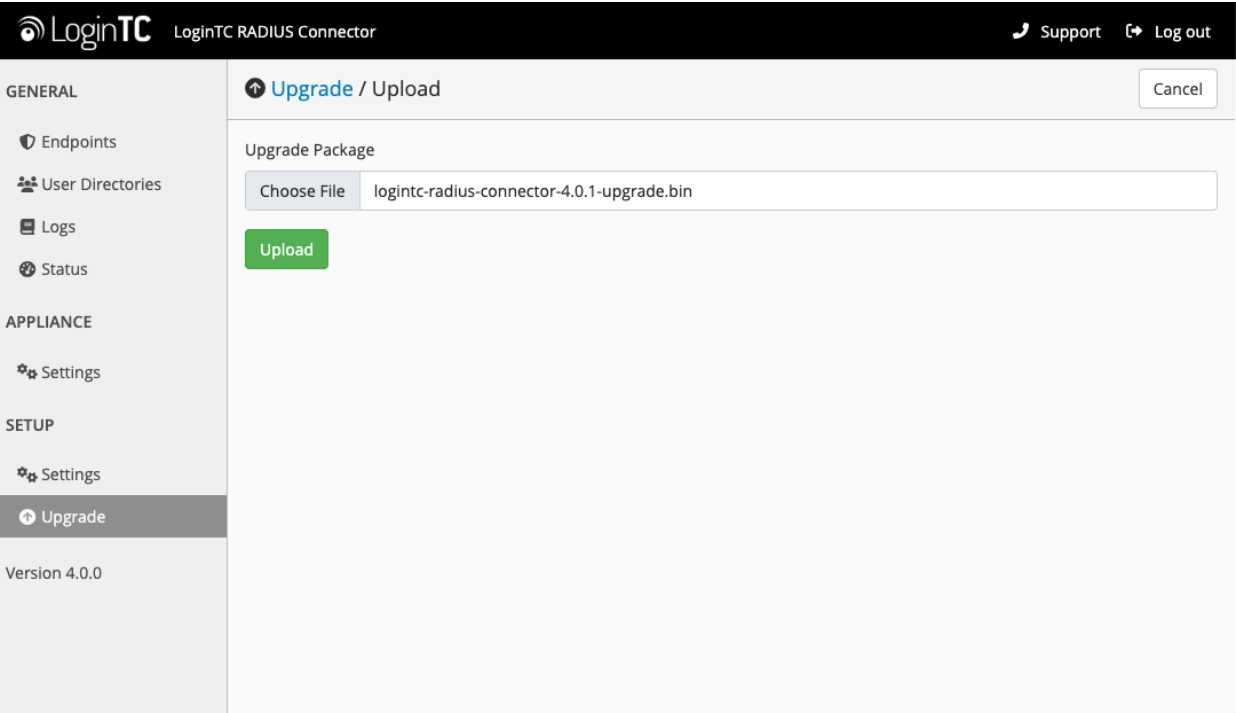
From 4.X

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

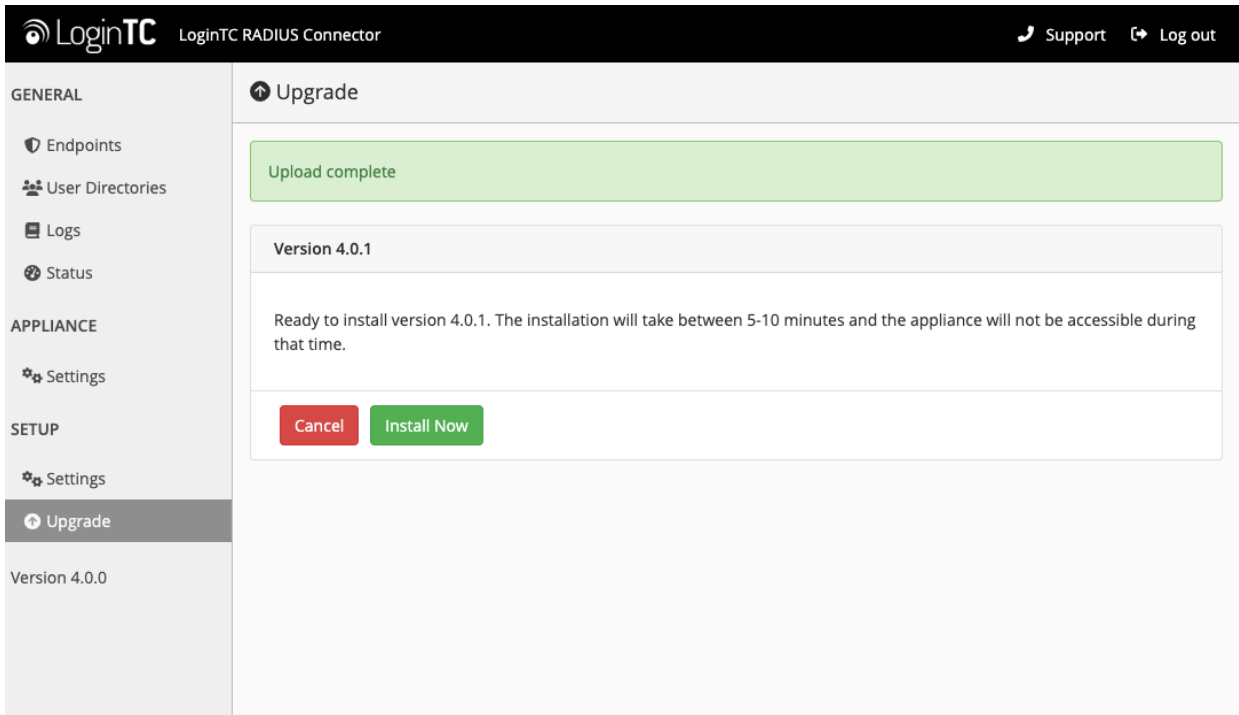
1. Navigate to **SETUP > Upgrade**:



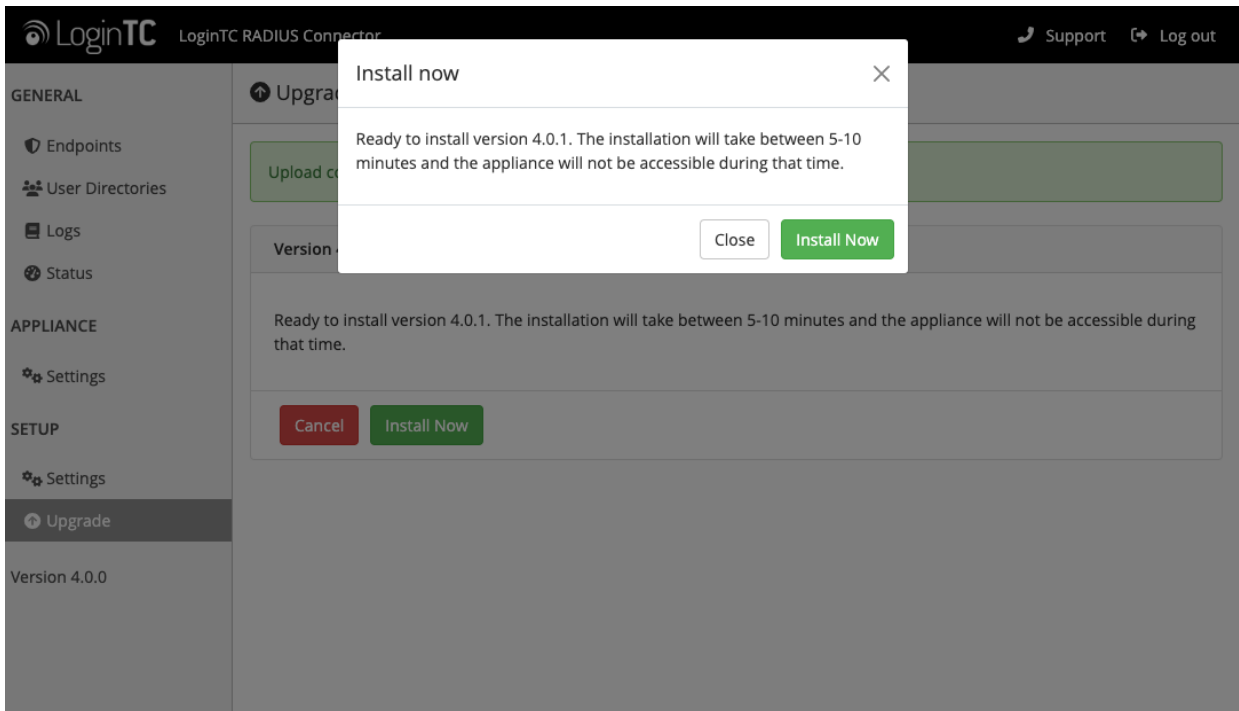
2. Click **Upload** and select your LoginTC RADIUS Connector upgrade file:



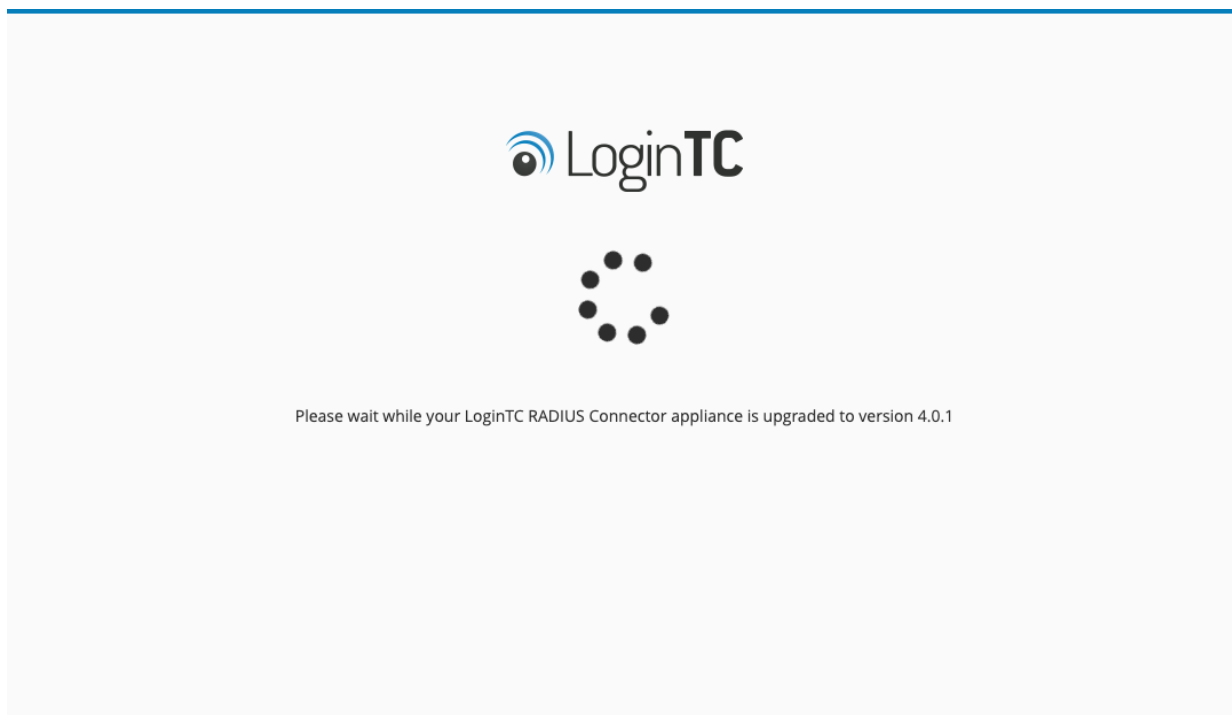
3. Click **Upload** and do not navigate away from the page:



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](#)