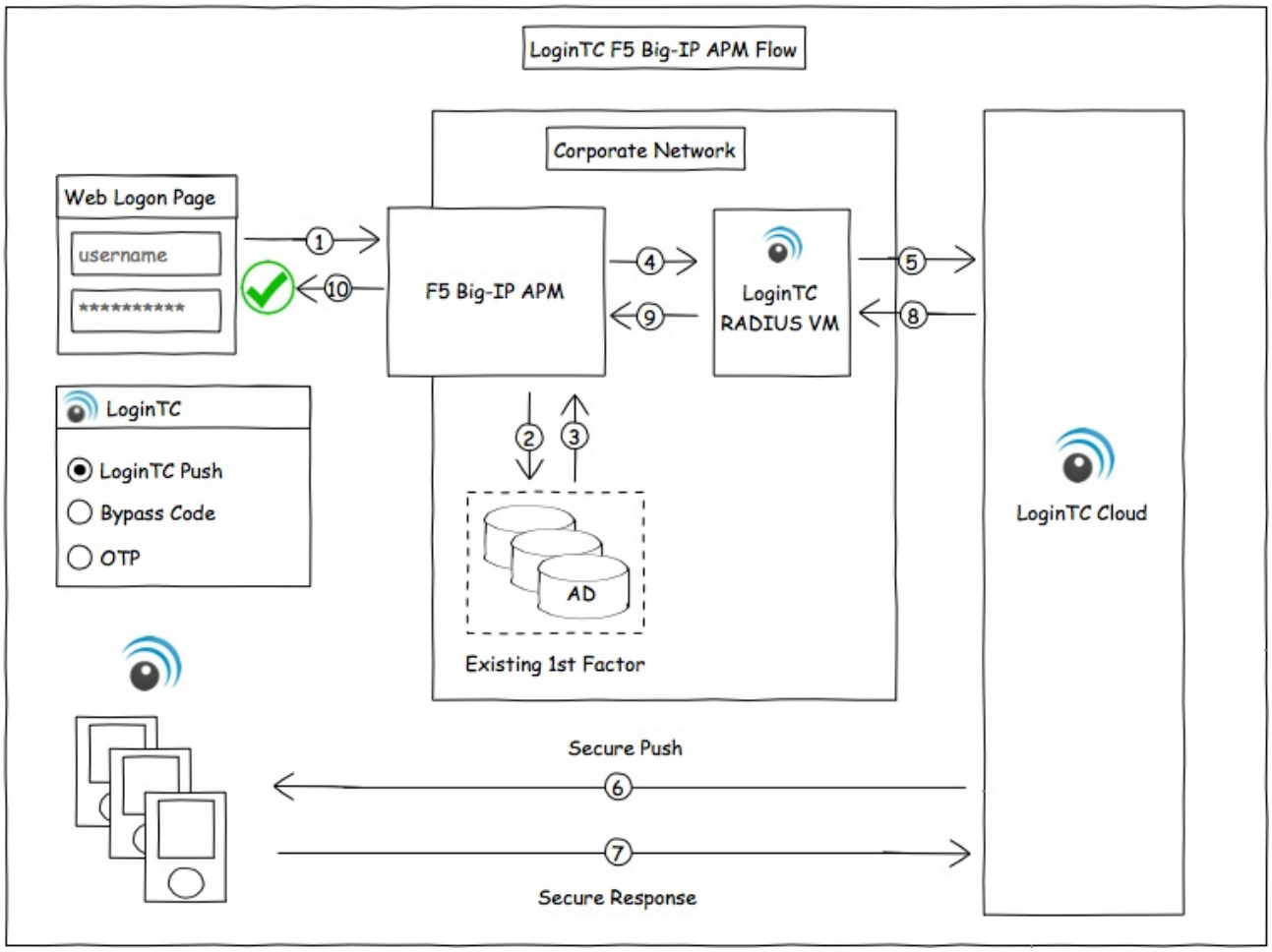
Two factor authentication for F5 BIG-IP APM

logintc.com/docs/connectors/f5.html

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.



Prerequisites

Before proceeding, please ensure you have the following:

LoginTC RADIUS Connector supported version: 2.5.0 or higher

In order to leverage the iframe based solution for F5 please upgrade to 2.5.0 or higher.

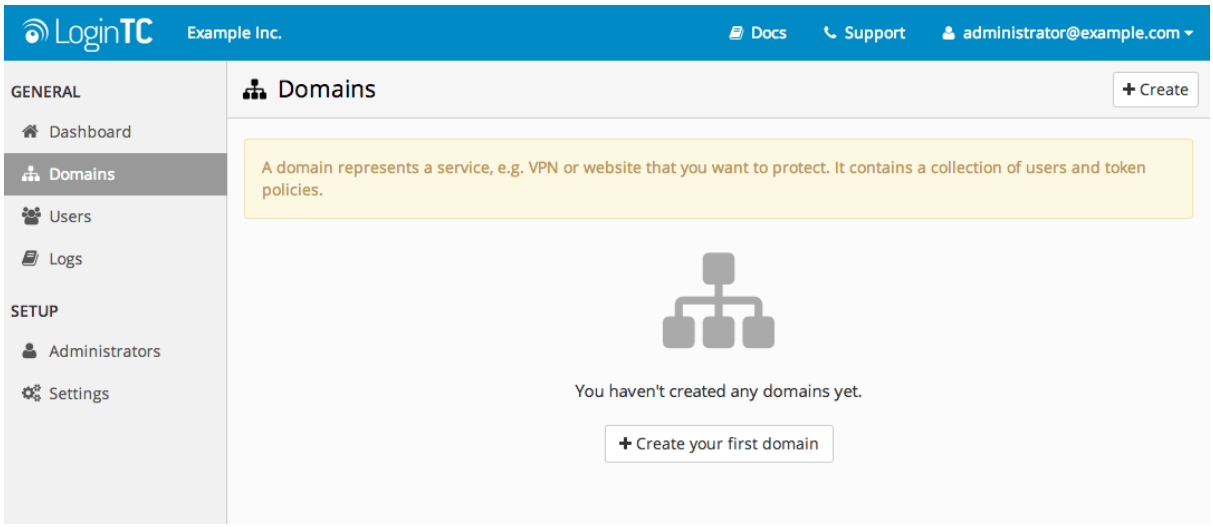
Subscription Requirement

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.

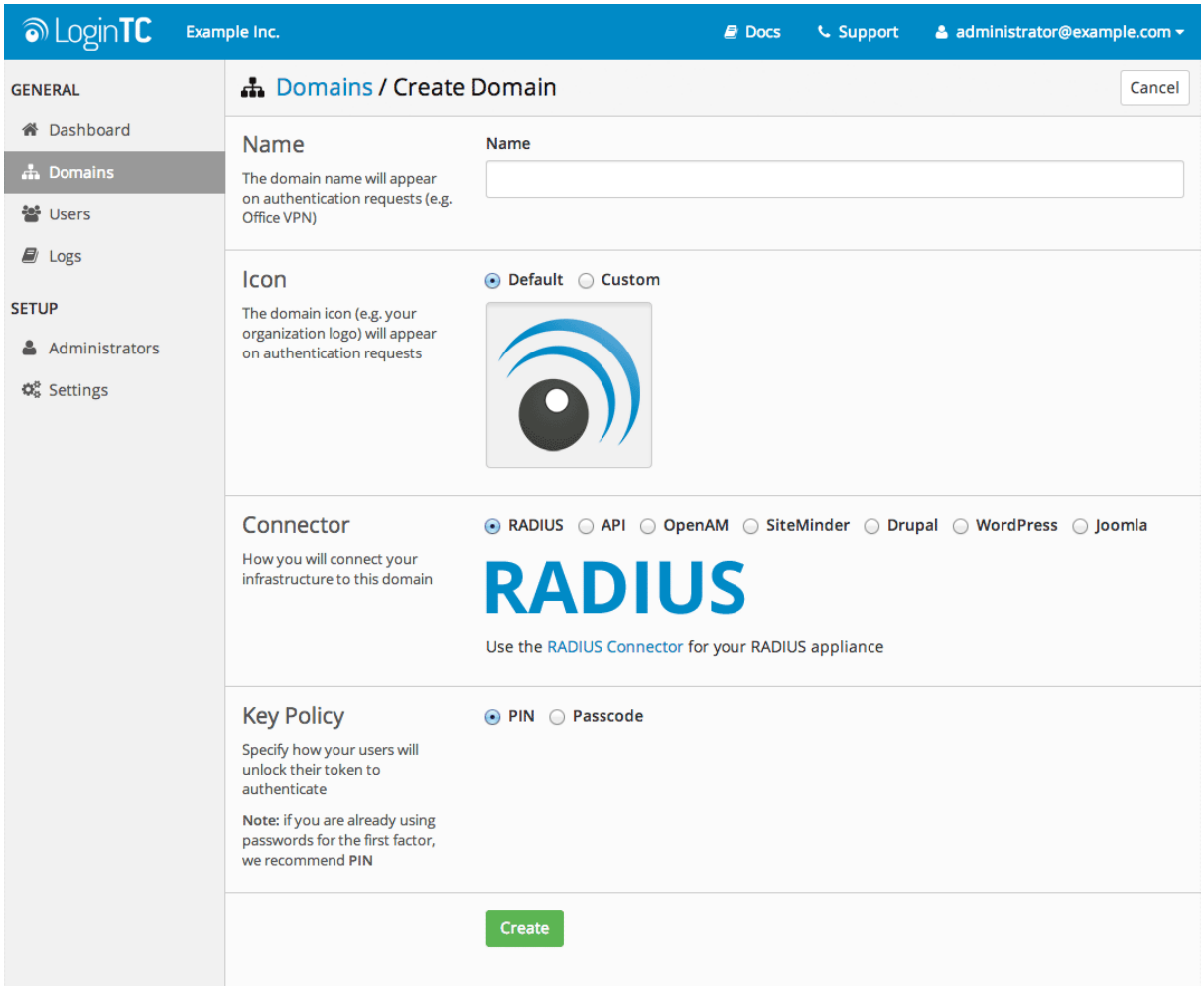
RADIUS Domain Creation

If you have already created a LoginTC Admin domain for your LoginTC RADIUS Connector, then you may skip this section and proceed to Installation.

1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Add Domain**:



4. Enter domain information:



Name
Choose a name to identify your LoginTC Admin domain to you and your users

Connector
RADIUS

Installation

The LoginTC RADIUS Connector runs CentOS 6.8 with SELinux. A firewall runs with the following open ports:

Port	Protocol	Purpose
22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
443	TCP	Web interface
80	TCP	Web interface
80	TCP	Package updates (outgoing)

Port	Protocol	Purpose
123	UDP	NTP, Clock synchronization (outgoing)

No incoming traffic rules required

The LoginTC RADIUS Connector is designed to work within your network without the need to change incoming rules on your firewall.

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 and will not be able to access the **web interface** unless it is changed.

The `logintc-user` has `sudo` privileges.

Configuration

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

1. LoginTC

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

2. First Factor

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 (since there are 4-digit PIN and Passcode options that unlock the tokens to access your domains, LoginTC-only authentication this still provides two-factor authentication).

3. 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 and Encryption

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

Data Encryption

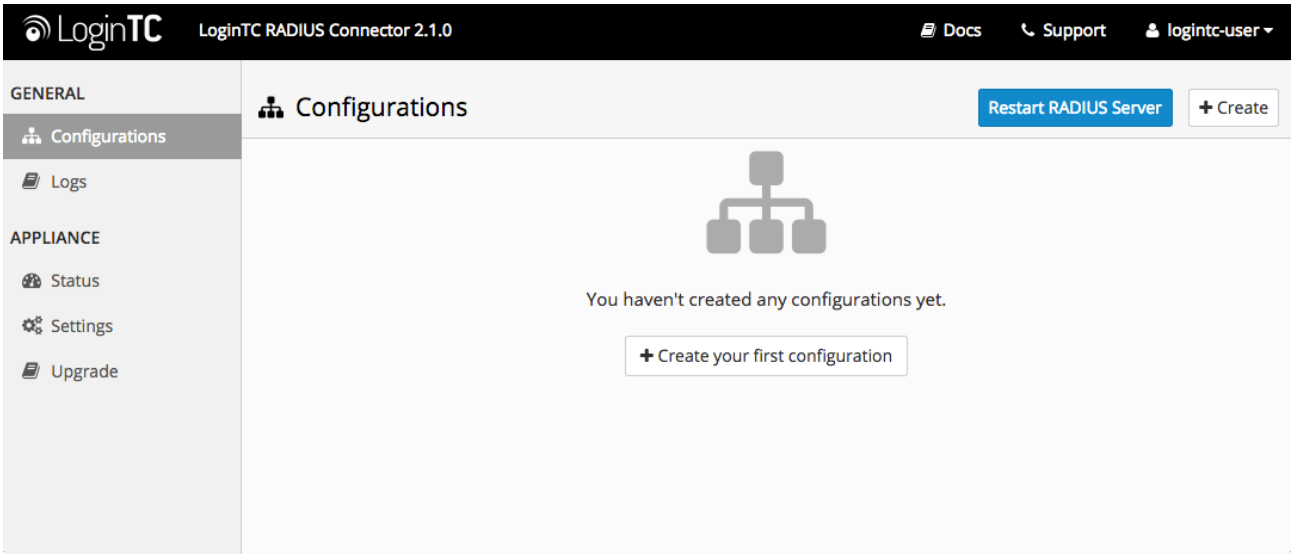
It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

The **web interface** makes setting up a configuration 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 Configuration

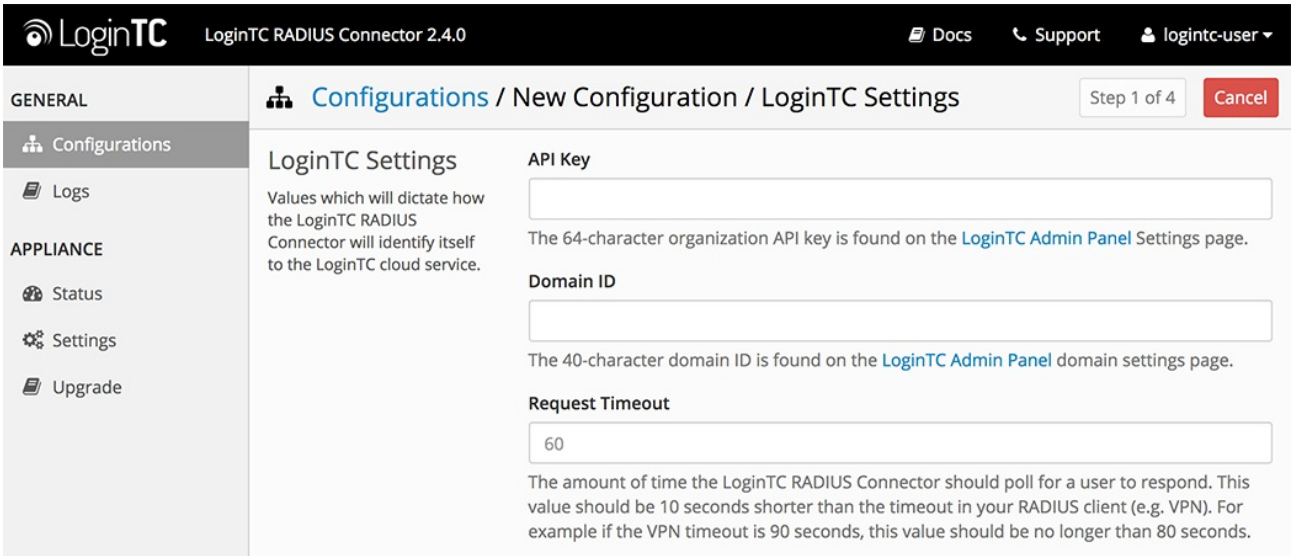
Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

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



LoginTC Settings

Configure which LoginTC organization and domain to use:

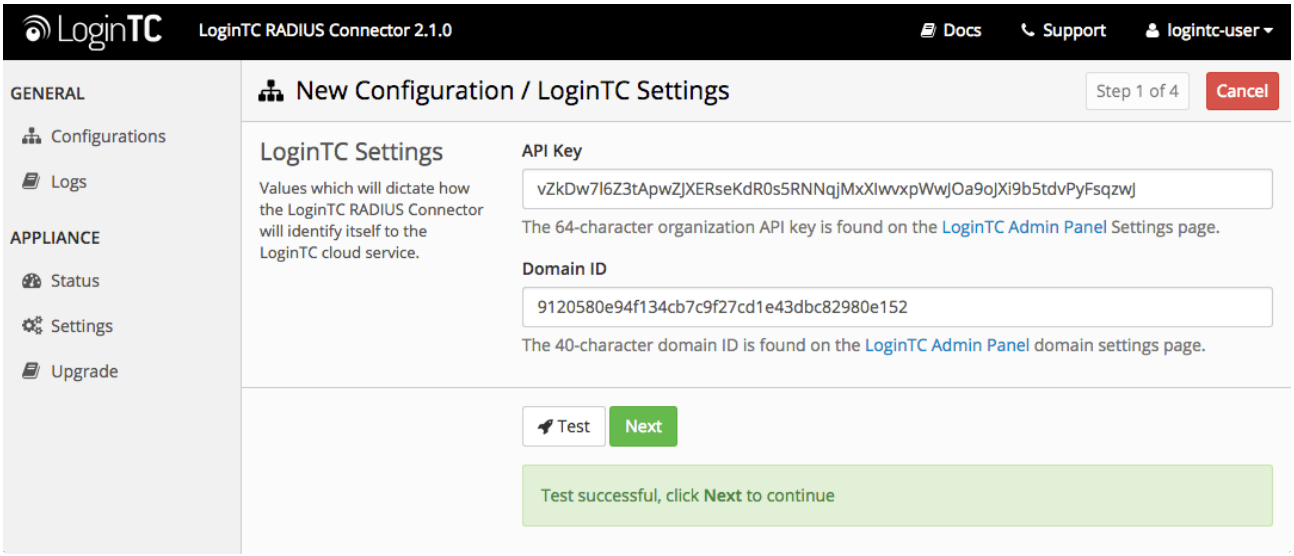


Configuration values:

Property	Explanation
`api_key`	The 64-character organization API key
`domain_id`	The 40-character domain ID

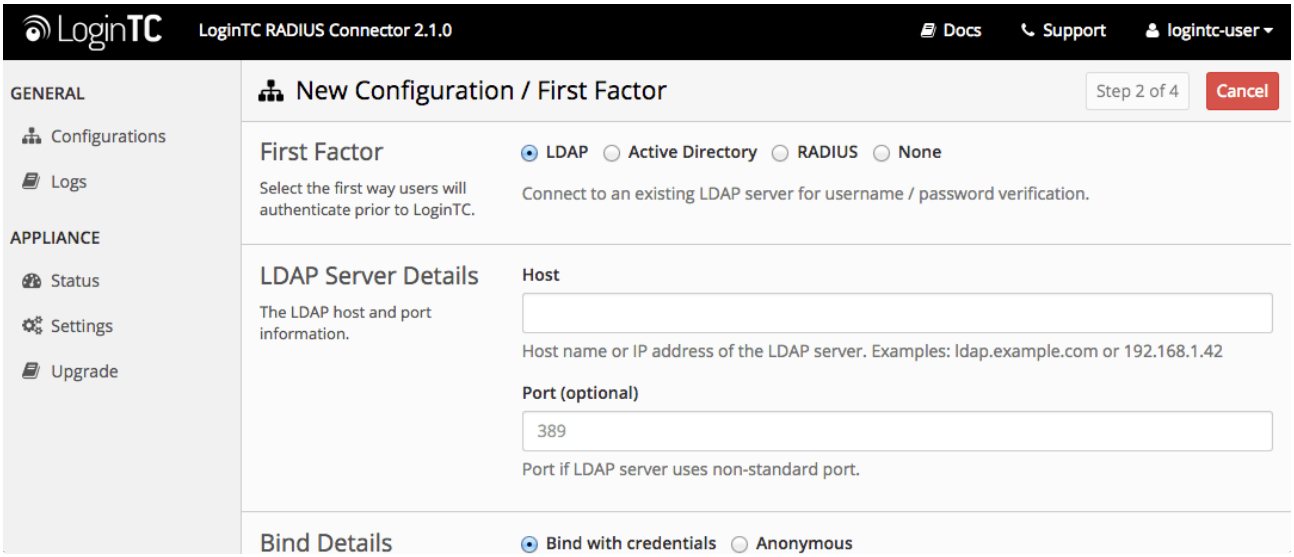
The API key is found on the LoginTC Admin Settings page. The Domain ID is found on your domain settings page.

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



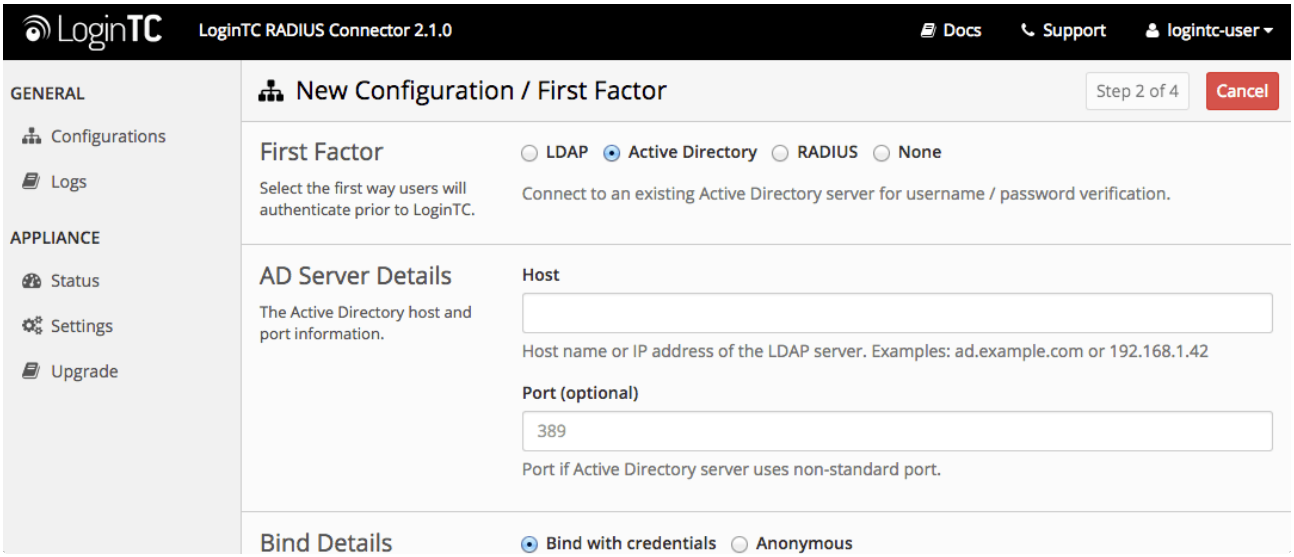
First Authentication Factor

Configure the first authentication factor to be used 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.



Active Directory / LDAP Option

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



Configuration values:

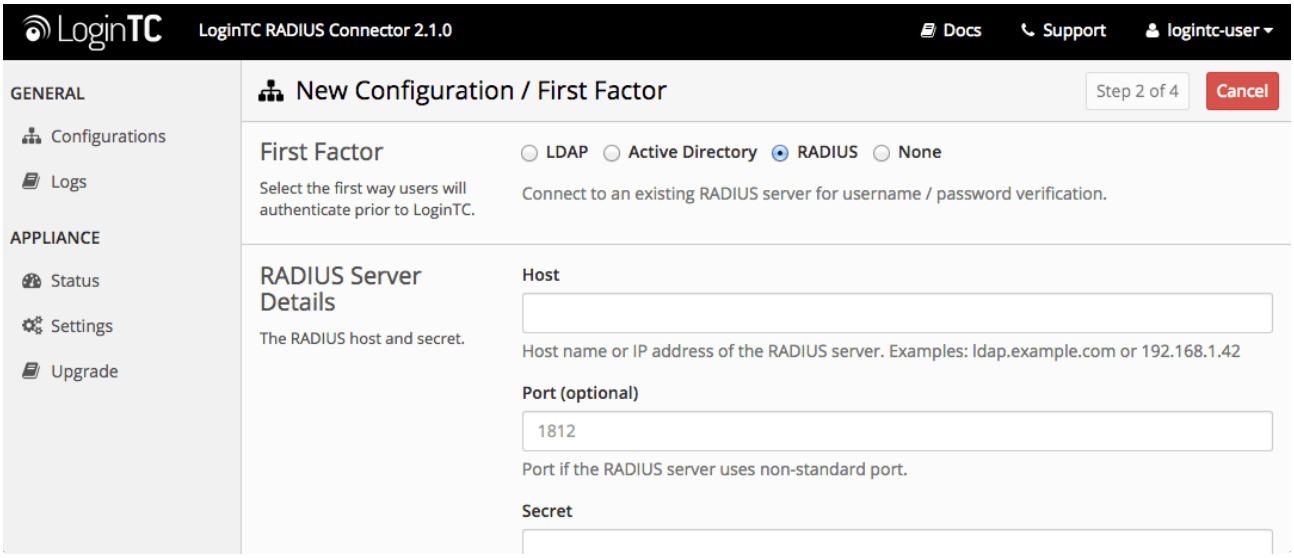
Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The 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
`attr_username`	The attribute containing the user's username	`sAMAccountName` or `uid`
`attr_name`	The attribute containing the user's real name	`displayName` or `cn`
`attr_email`	The attribute containing the user's email address	`mail` or `email`
`Group Attribute` (optional)	Specify an additional user group attribute to be returned the authenticating server.	`4000`
`RADIUS Group Attribute` (optional)	Name of RADIUS attribute to send back	`Filter-Id`
`LDAP Group` (optional)	The name of the LDAP group to be sent back to the authenticating server.	`SSLVPN-Users`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

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**:



Configuration values:

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

RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) found in the FreeRADIUS dictionary files will be relayed.

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

Passthrough

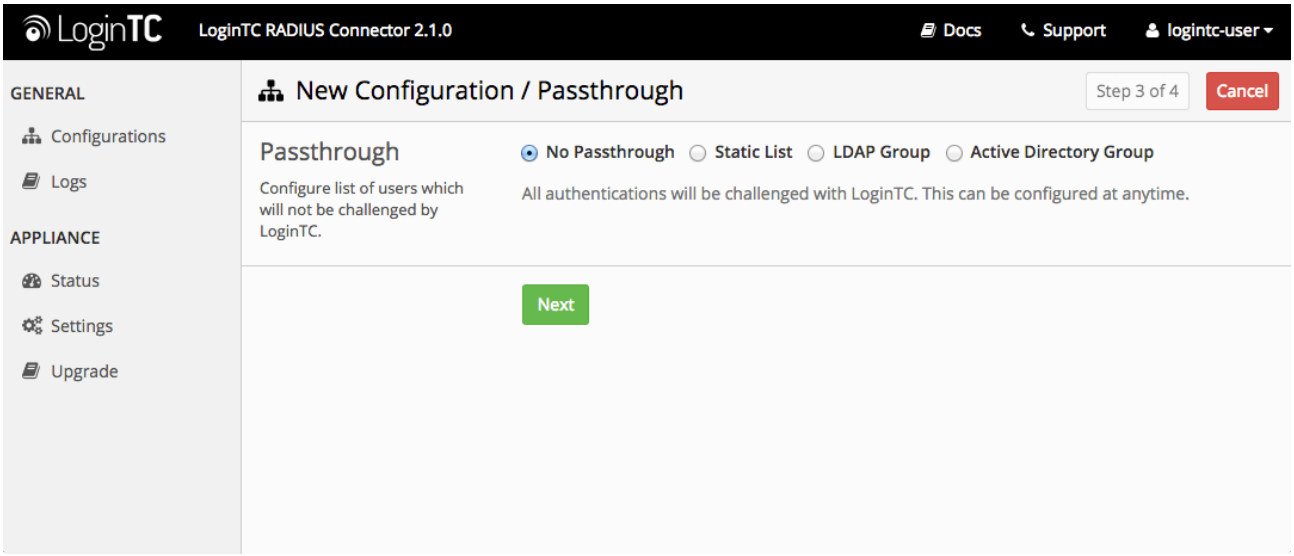
Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

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.

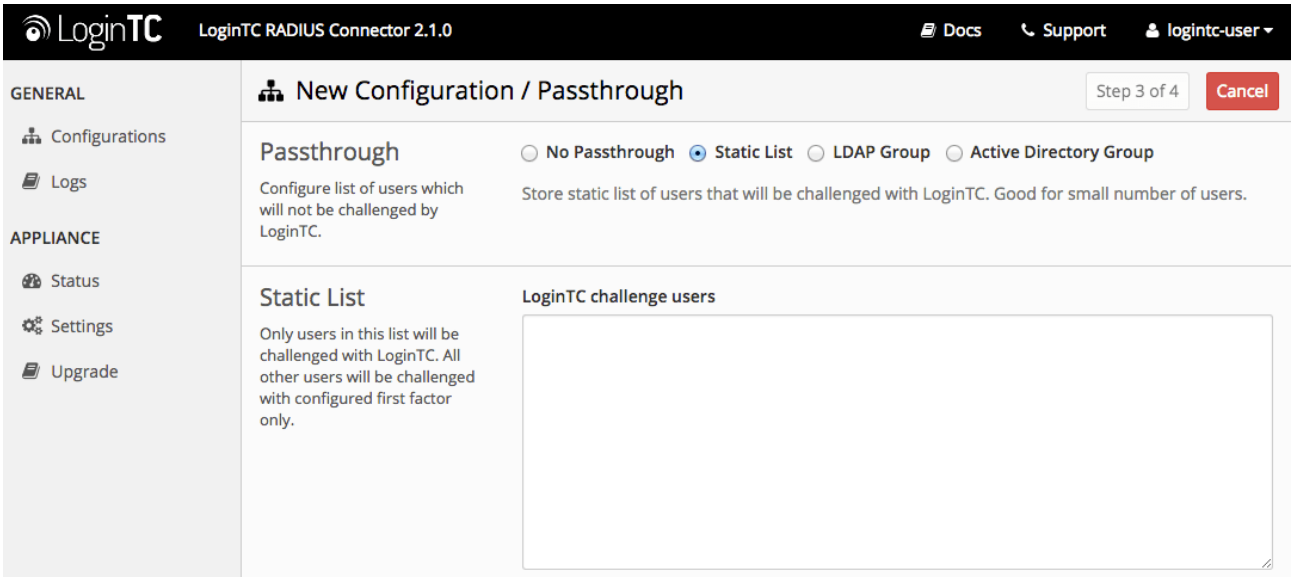
No Passthrough (default)

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



Static 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.

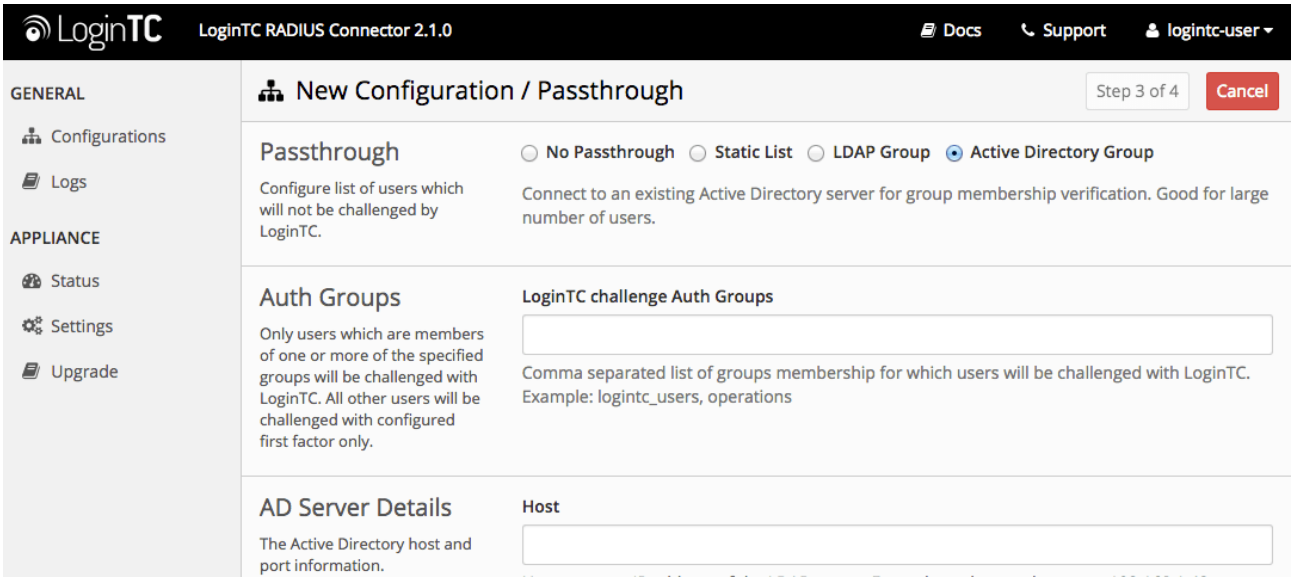


LoginTC challenge users: a new line separated list of usernames. For example:

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

Active Directory / LDAP Group

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
`LoginTC challenge auth groups`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users` or `two-factor-users`

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`
`attr_username`	The attribute containing the user's username	`sAMAccountName` or `uid`
`attr_name`	The attribute containing the user's real name	`displayName` or `cn`
`attr_email`	The attribute containing the user's email address	`mail` or `email`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

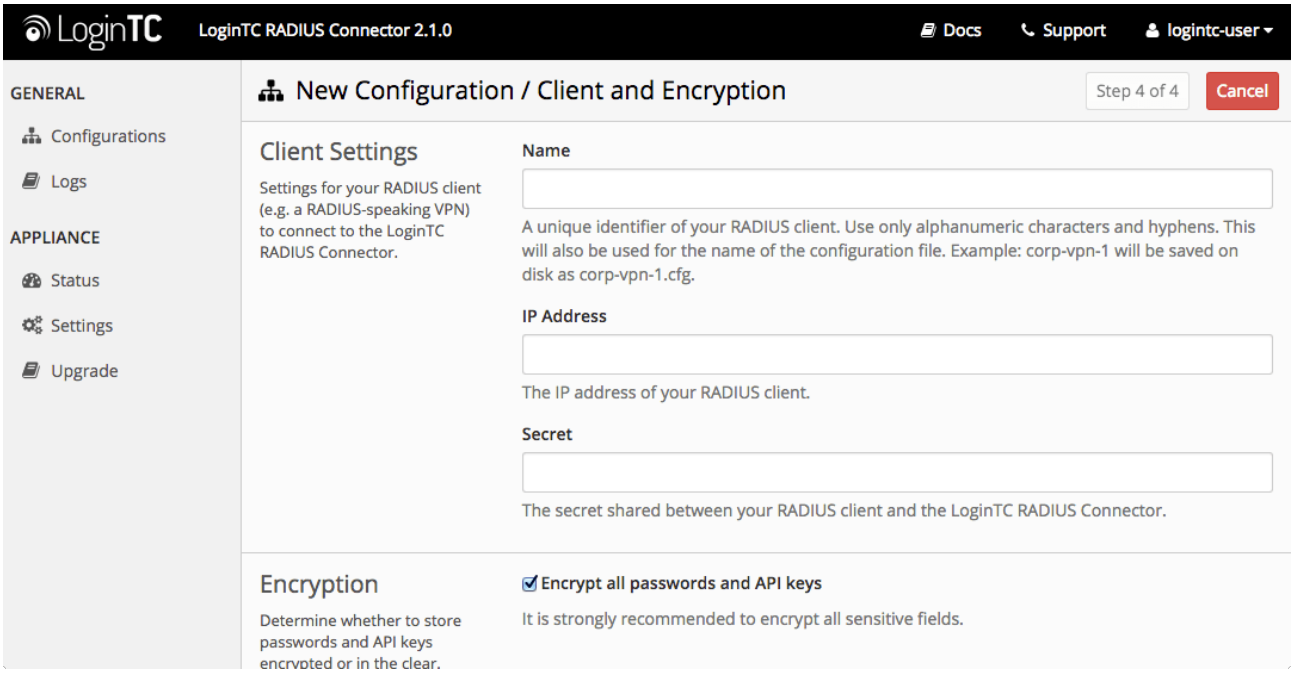
Configuration Simplified

If Active Directory / LDAP Option was selected in First Authentication Factor the non-sensitive values will be pre-populated to avoid retyping and potential typos.

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

Client and Encryption

Configure RADIUS client (e.g. your F5):



Client configuration values:

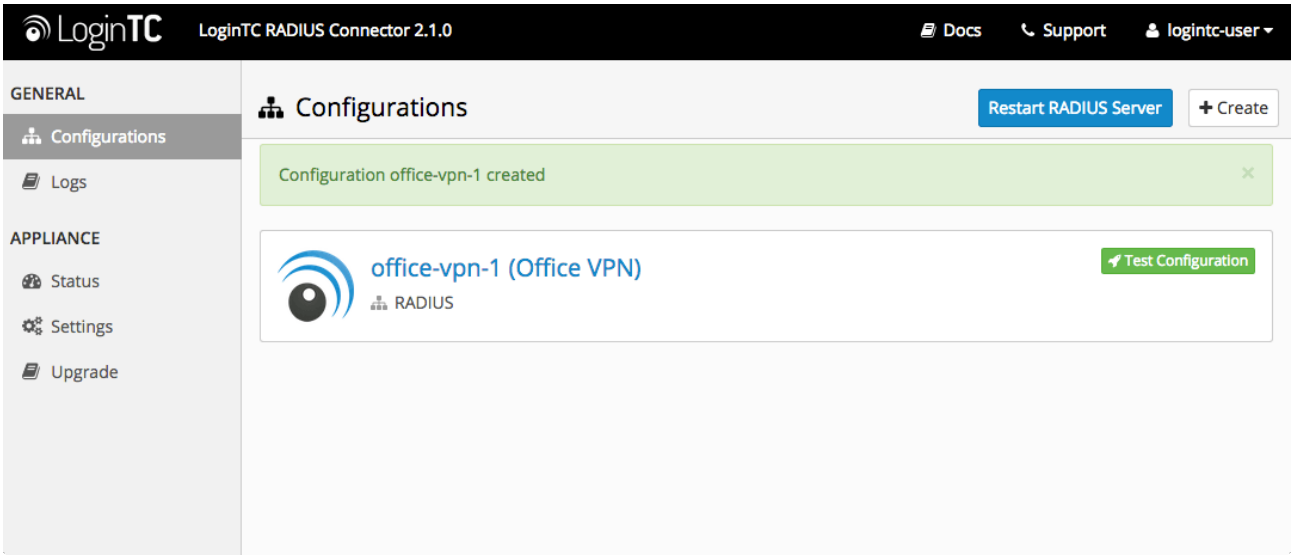
Property	Explanation	Examples
`name`	A unique identifier of your RADIUS client	`CorporateVPN`
`ip`	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	`192.168.1.44`
`secret`	The secret shared between the LoginTC RADIUS Connector and its client	`bigsecret`

The `Authenticate Mode` must be set to `Iframe`.

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

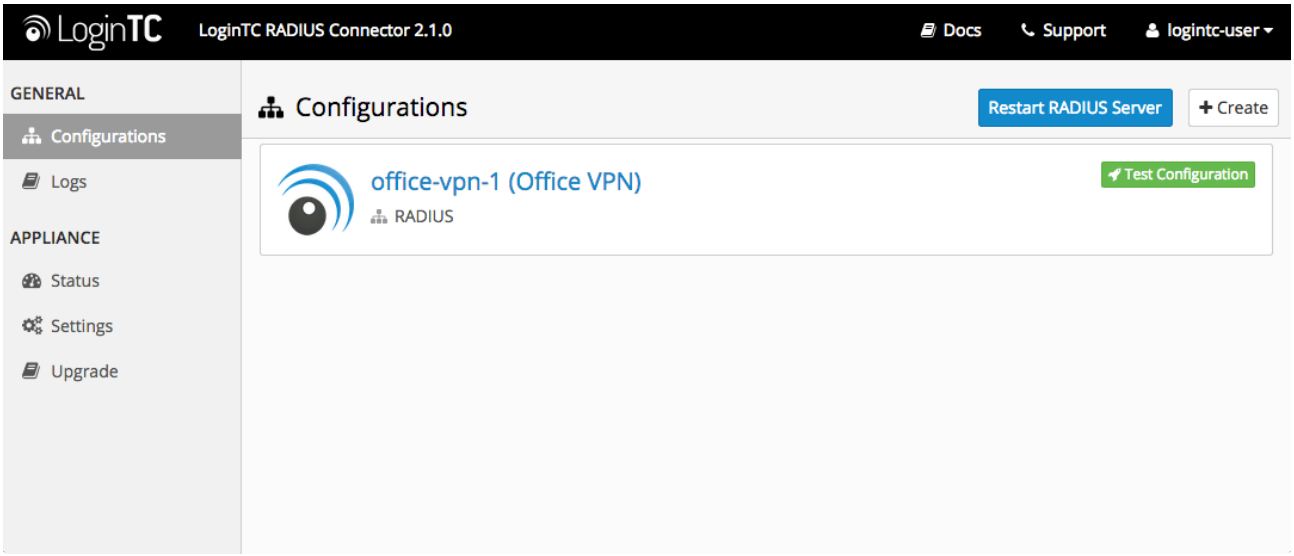
Click **Test** to validate the values and then click **Save**.



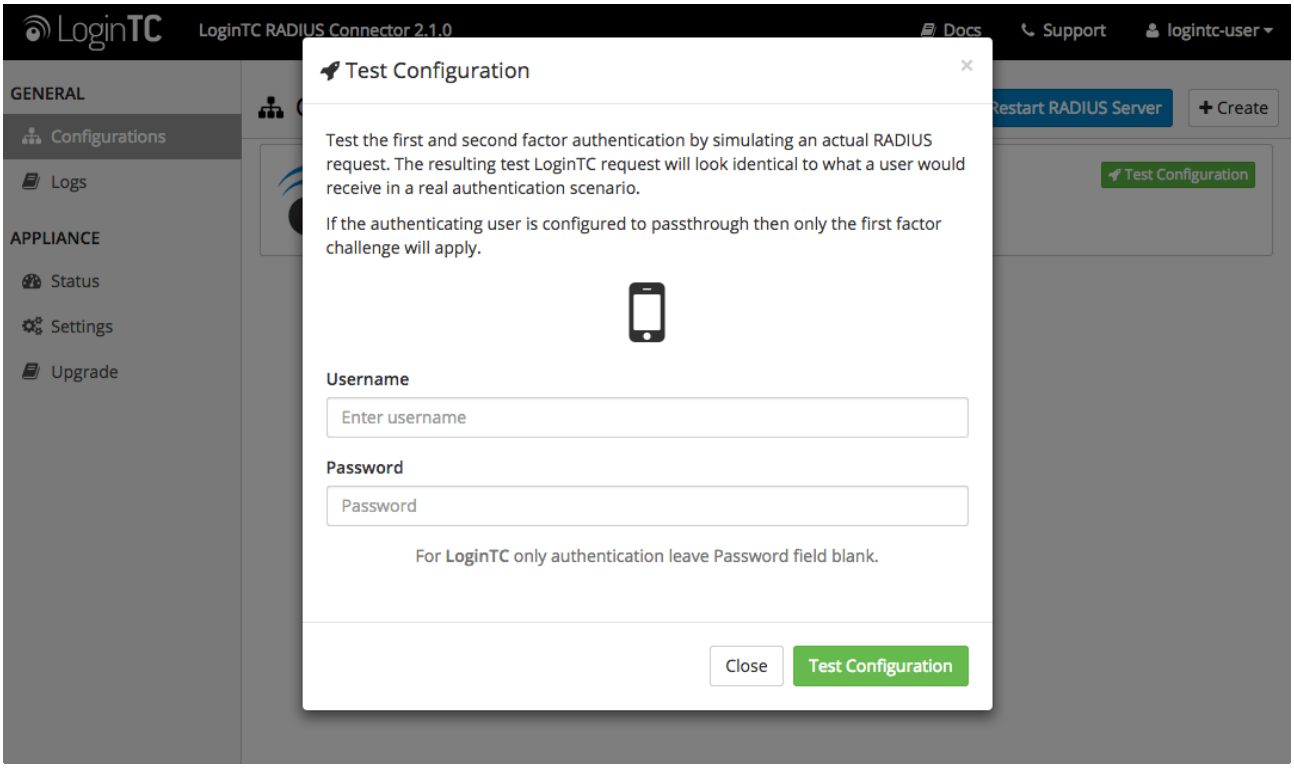
Testing

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:

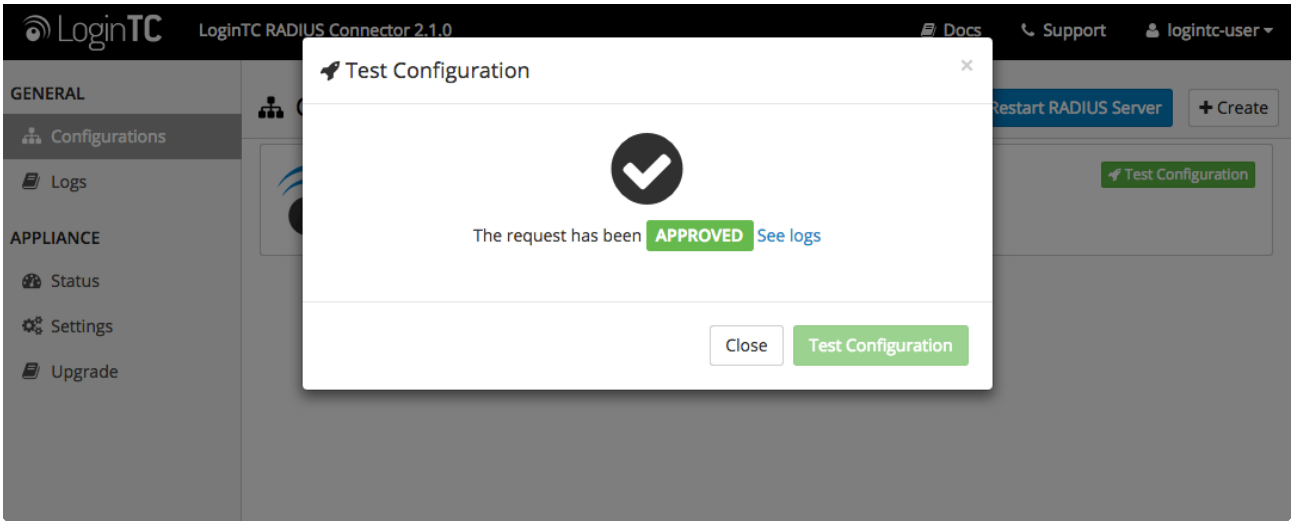
When you have loaded a token for your new user and domain, navigate to your appliance**web interface** URL:



Click **Test Configuration**:

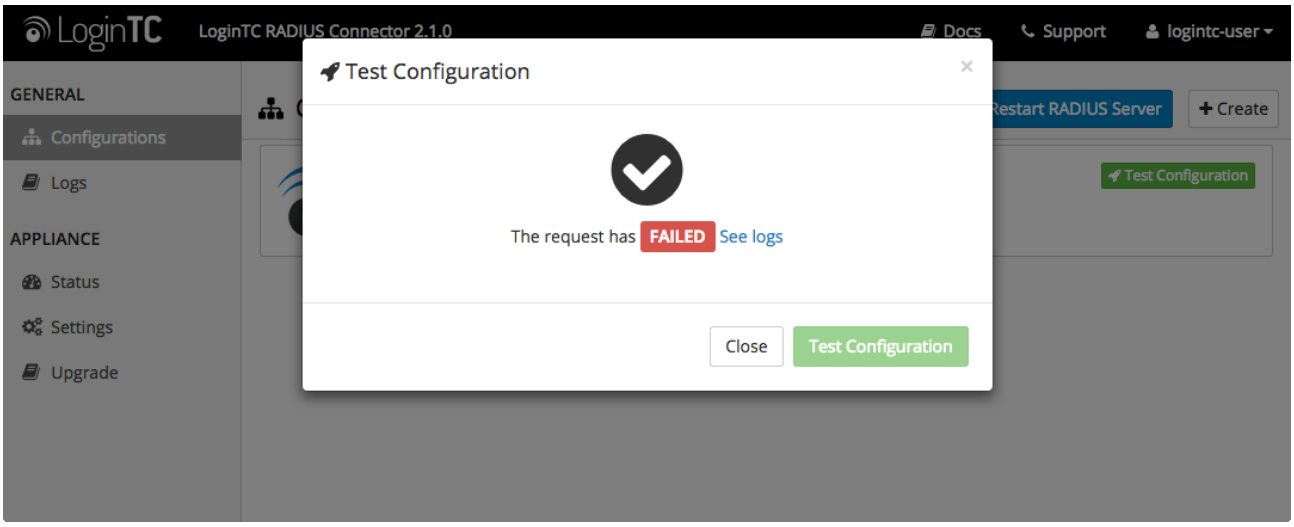


Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

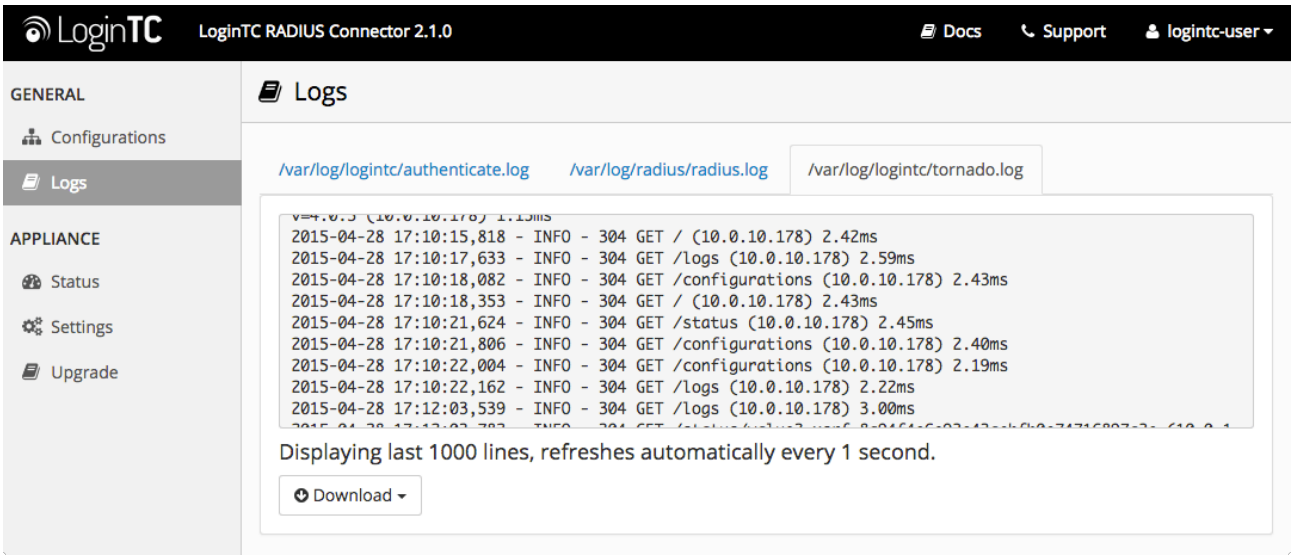


Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

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



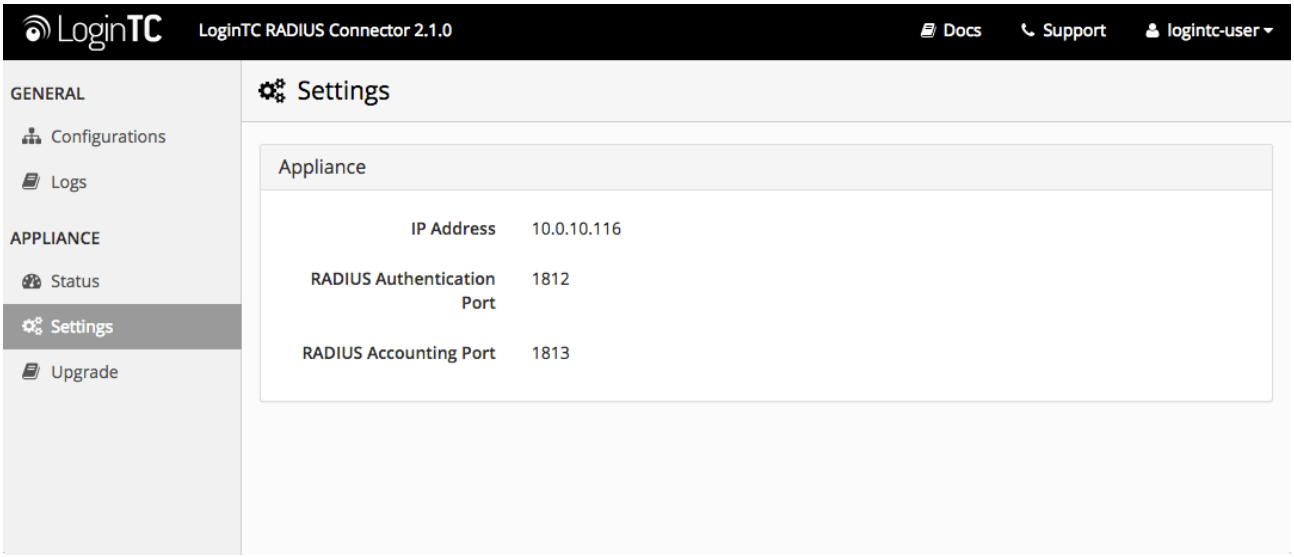
In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:



F5 Big-IP APM Configuration - Quick Guide

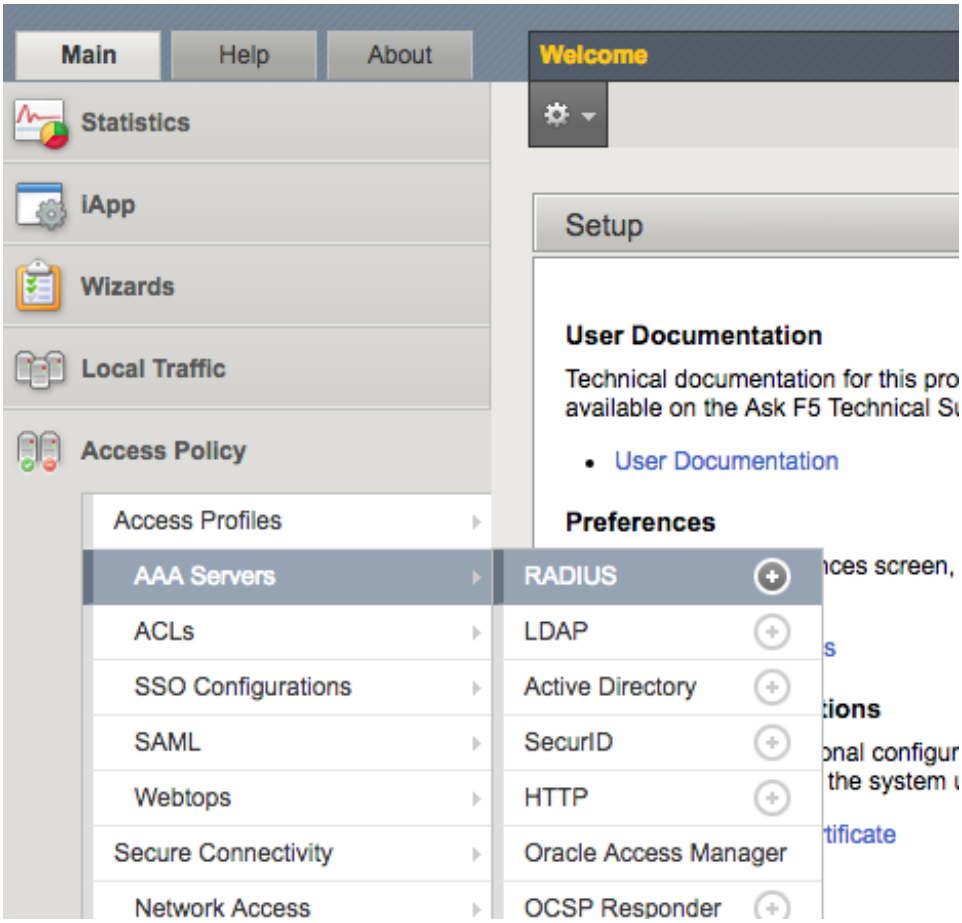
Once you are satisfied with your setup, configure your F5 Big-IP APM to use the LoginTC RADIUS Connector.

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

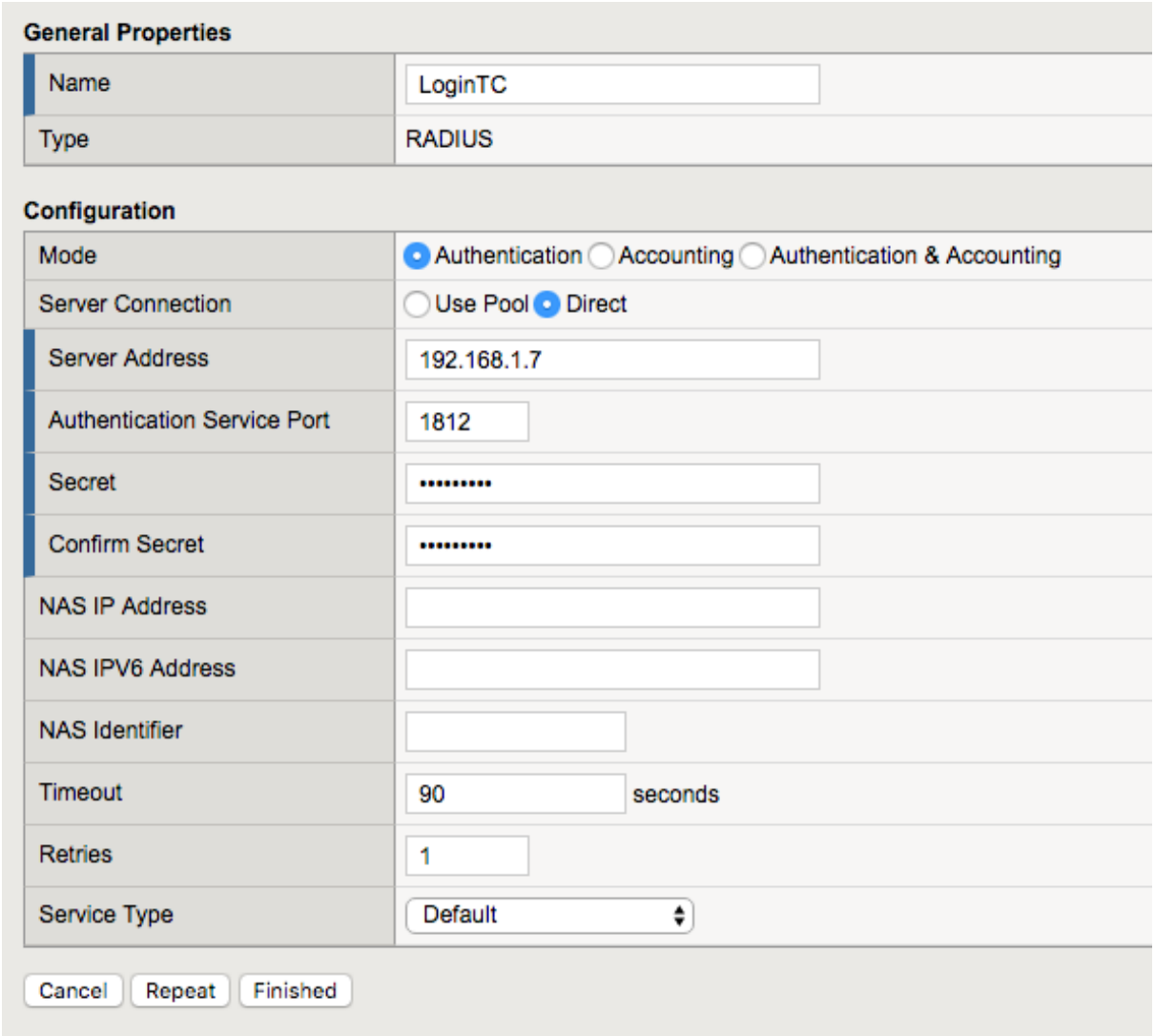


The following are quick steps to setup F5 Big-IP APM with LoginTC.

1. Log into the F5 Big-IP Configuration Utility / Management Console
2. Navigate to **Access Policy** > **AAA Severs** > **RADIUS**:



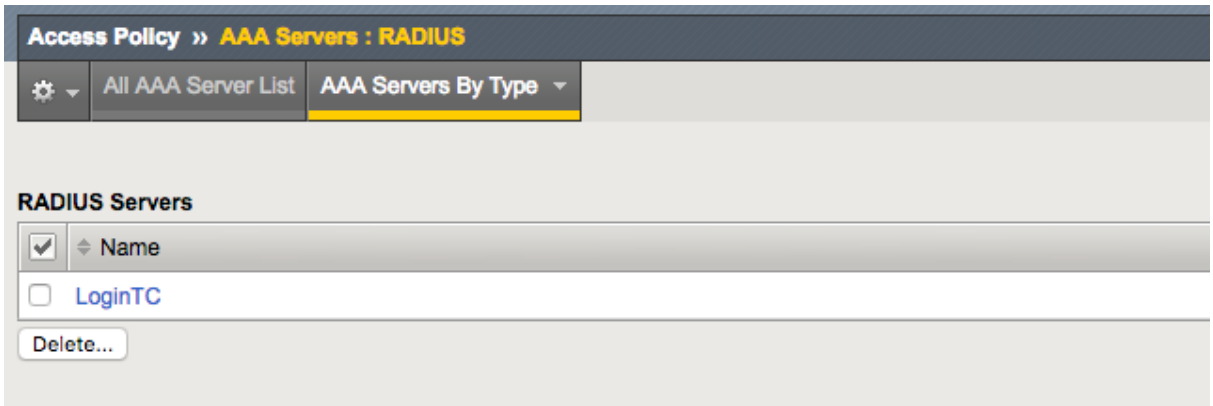
3. Click **Create…**



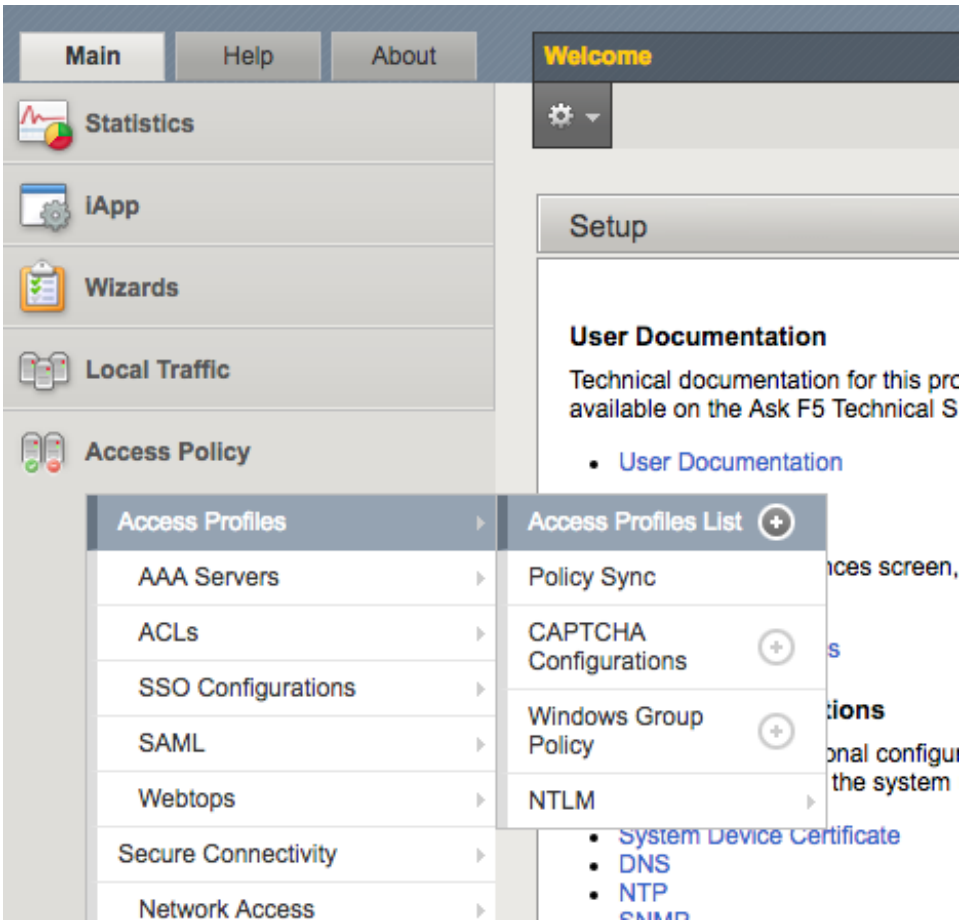
Property	Explanation	Example
`Name`	The name of this configuration.	`LoginTC`
`Mode`	The method in which F5 will leverage the LoginTC RADIUS Connector. Must be Authentication.	`Authentication`
`Server Connection`	The type of connection, either Use Pool or Direct. Use Pool can be leveraged for failover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

Property	Explanation	Example
`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**

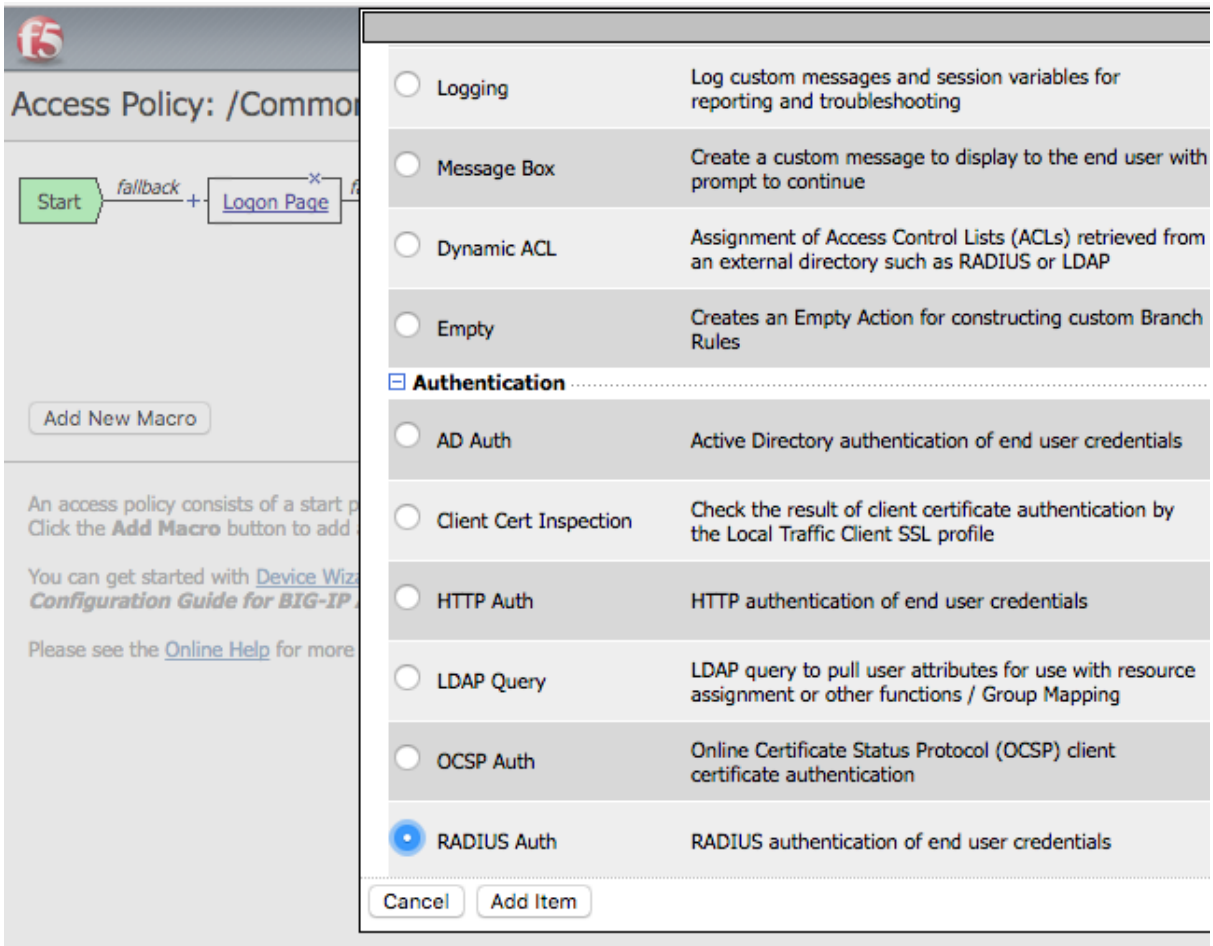


5. Modify an existing Access Policy or create an new one to leverage the newly defined RADIUS server pointing to the LoginTC RADIUS Connector.
6. Navigate to **Access Policy** > **Access Profiles** > **Access Profiles List**:

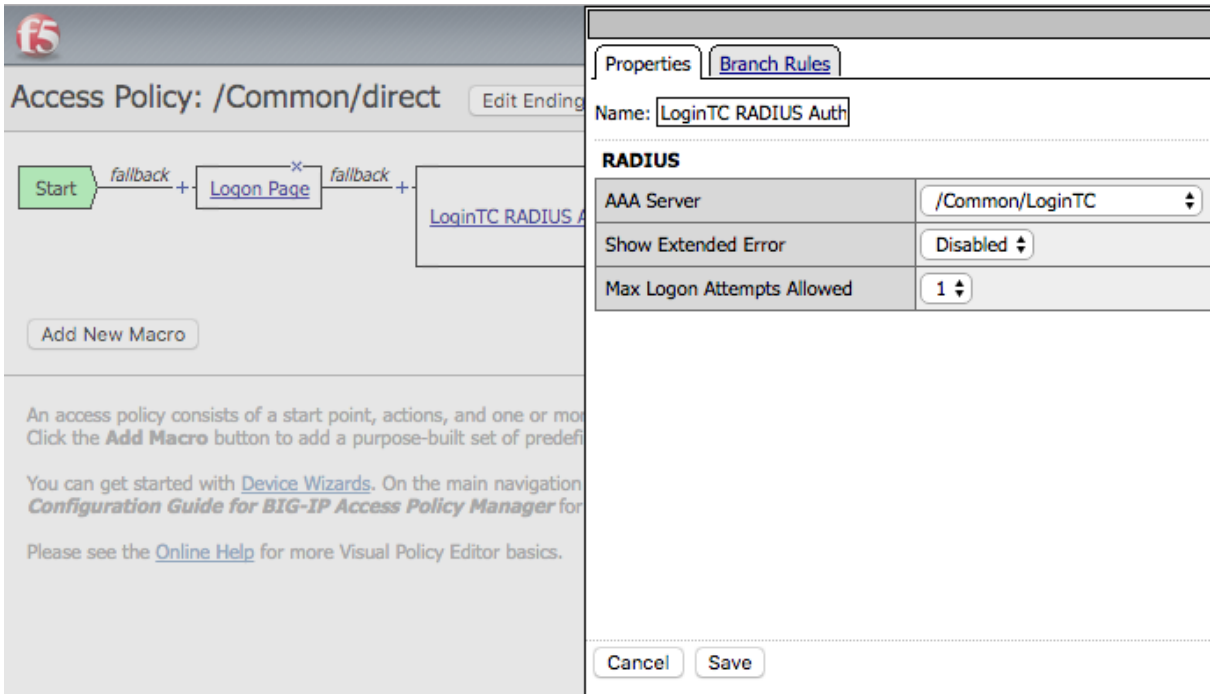


7. For the Access Profile you wish to edit click **Edit…**.

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

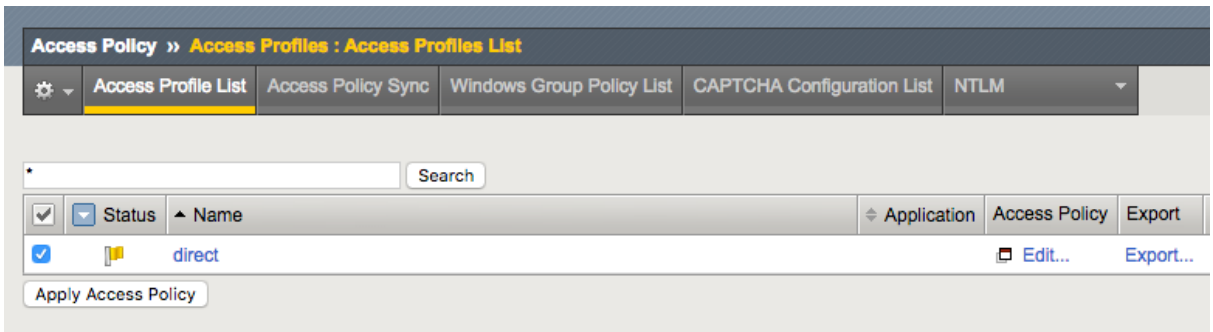


9. Fill in the configuration details and click **Save**:

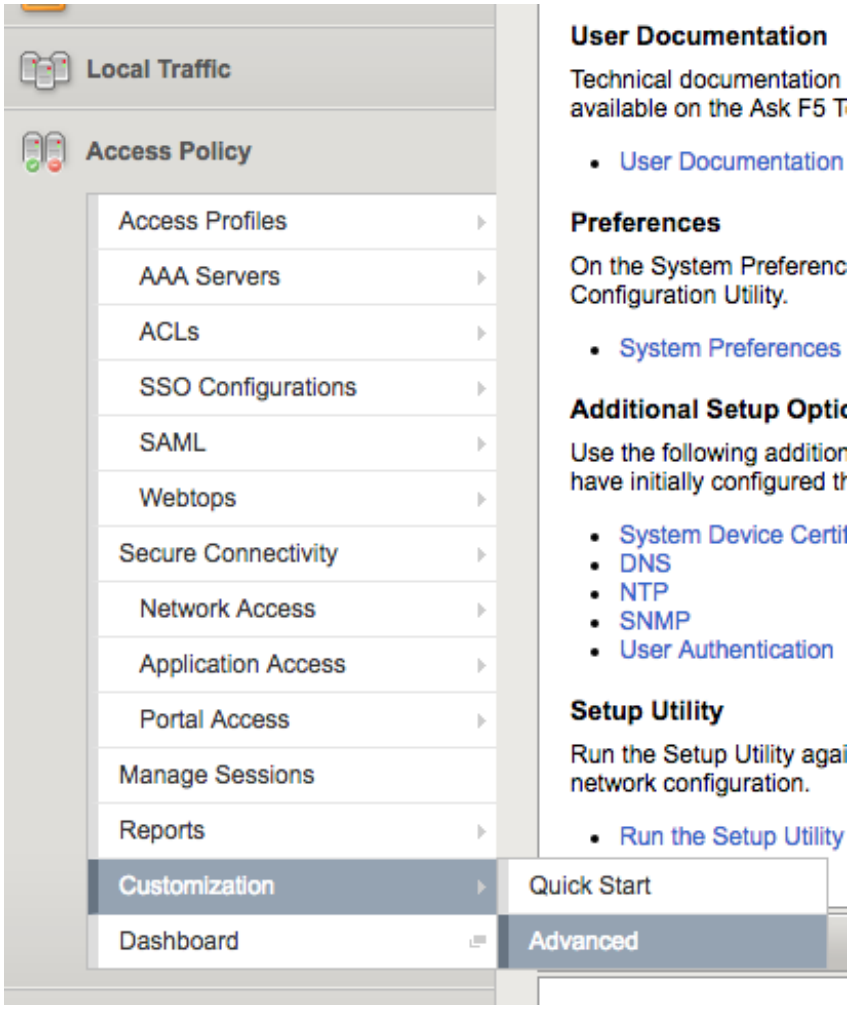


Property	Explanation	Example
`Name`	The name of this Access Policy Item.	`LoginTC RADIUS Auth`
`AAA Server`	The AAA Server to leverage. Must be the one created in Step 3.	`LoginTC`
`Show Extended Error`	Displays comprehensive error messages generated by the authentication server. Must be Disabled.	`Disabled`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

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

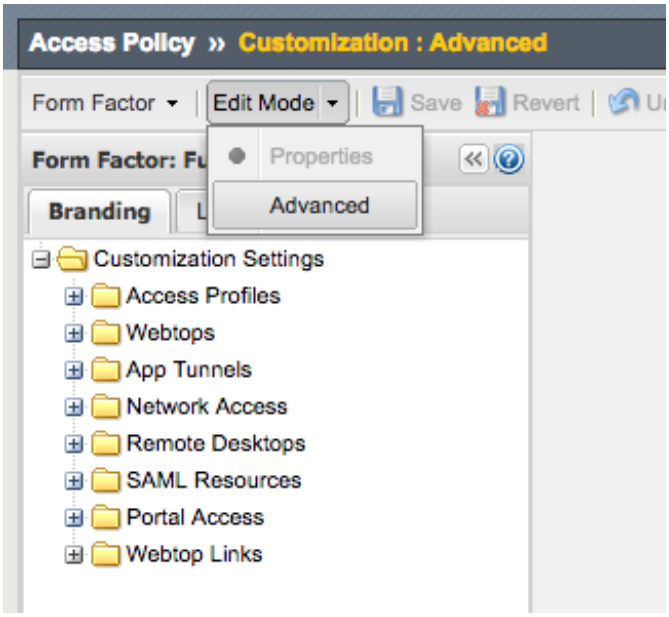


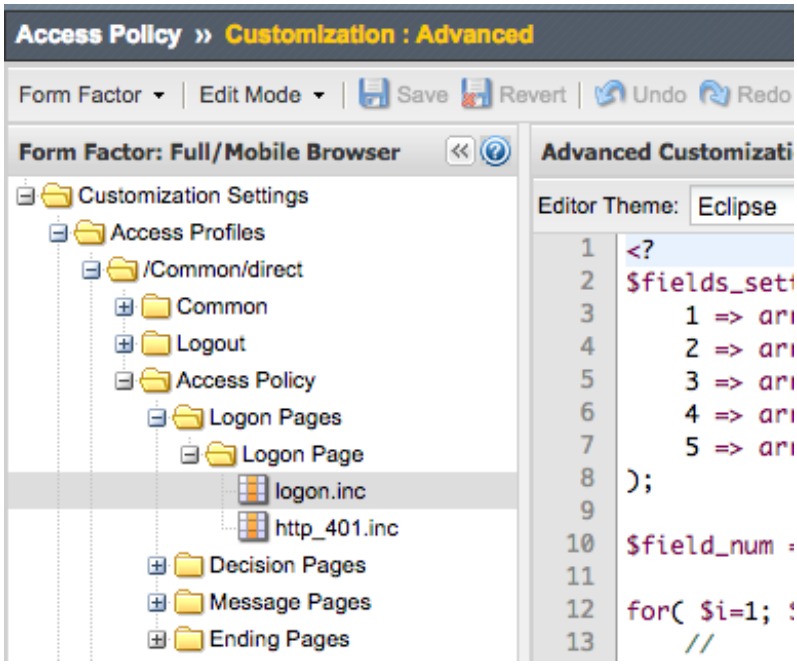
12. Navigate to **Access Policy** > **Customization** > **Advanced**:



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 `Domain ID` (https://www.logintc.com/downloads/f5-code-snippet-v1.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_domain_id = 'YOUR_DOMAIN_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-v1.js",document.getElementsByTagName("head")
[0].appendChild(e)}else document.documentElement.className=""});
    </script>
    <!-- End of LoginTC F5 Integration -->
```

Note: Add your Domain ID

Replace `YOUR_DOMAIN_ID` with the actual LoginTC domain ID you wish to use.

17. Add the edited snippet before `</head>`;

```
<!-- 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_domain_id = '9120580e94f134cb7c9f27cd1e43dbc82980e152';

    document.documentElement.className="logintc";var domReady=function(e,n,t){n=document
</script>
<!-- End of LoginTC F5 Integration -->

</head>
```

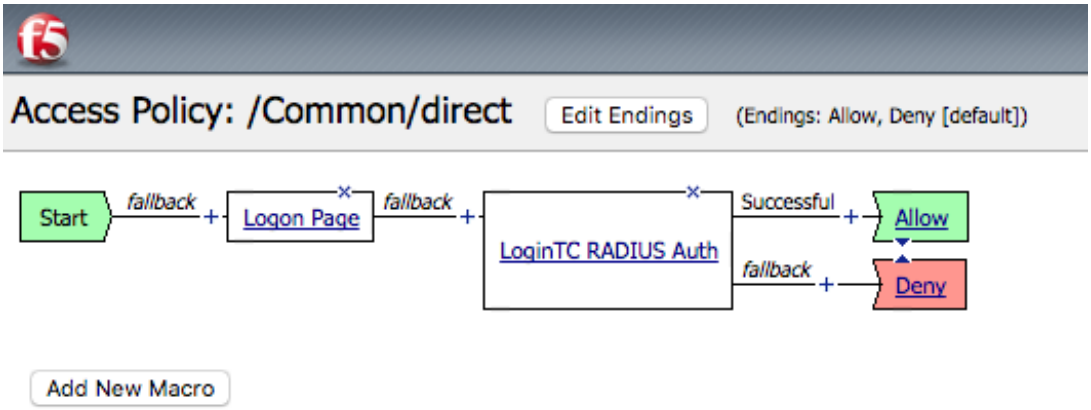
18. Click **Save Draft** > **Yes** > **Save**:

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

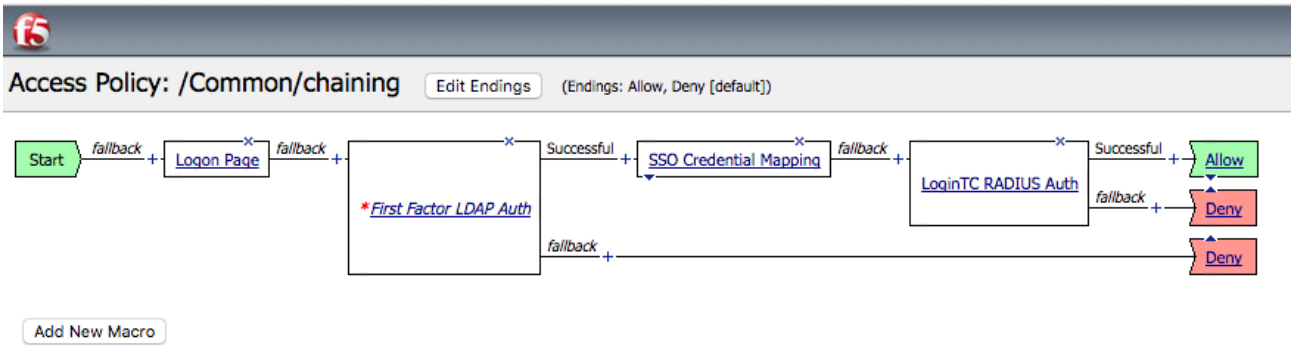
20. On the Access Profiles List the profile just modified will be flagged with a yellow flag. Select it and click **Apply Access Policy**.

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:



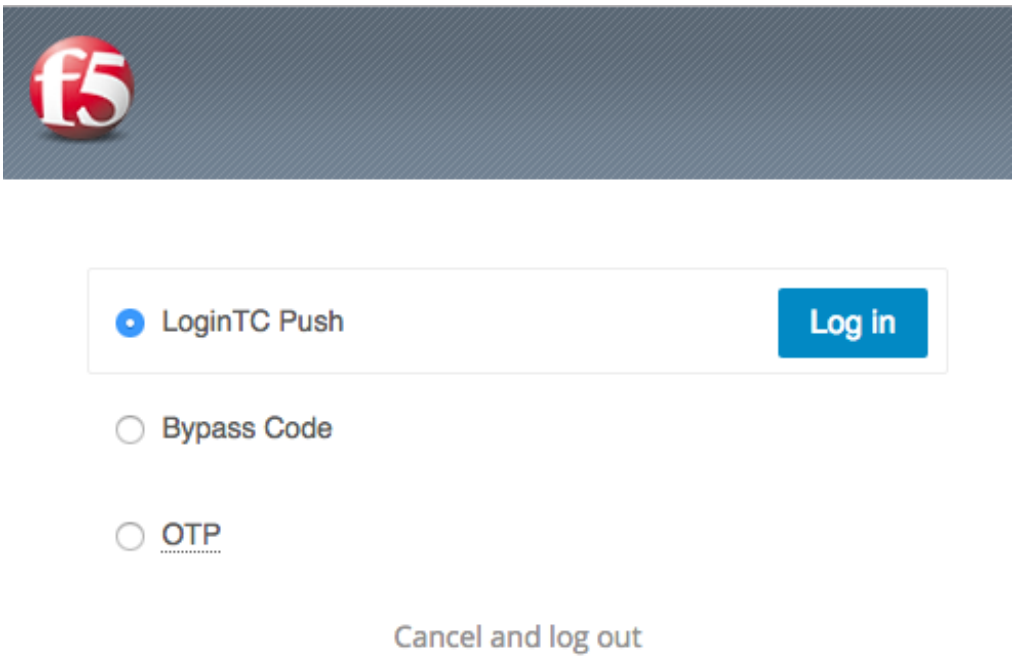
Chaining the LoginTC RADIUS Connector:



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.

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:



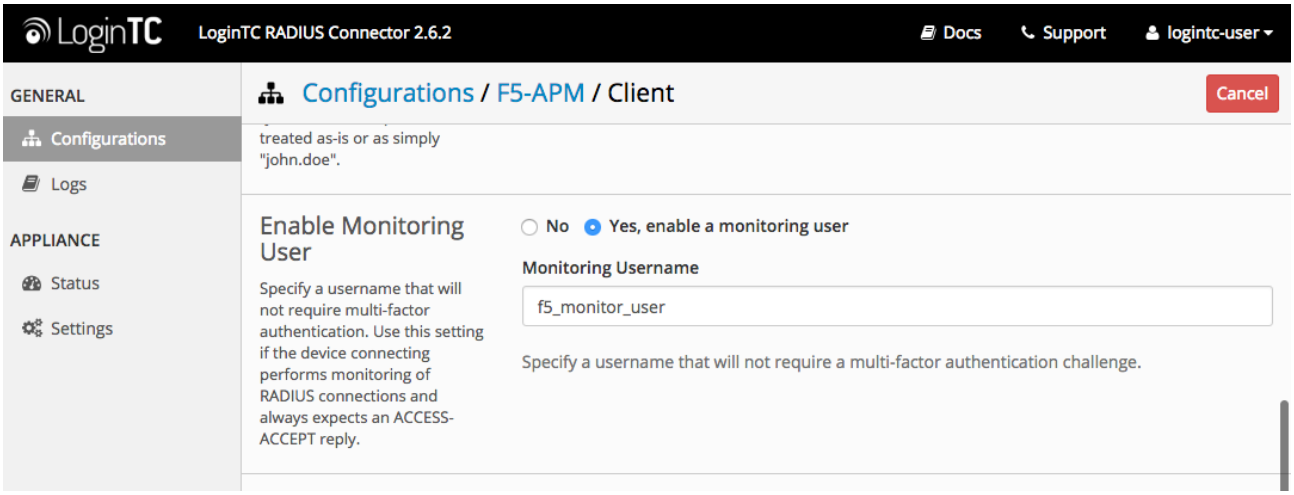
Select the method you wish to use to authenticate and continue.

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**



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 domain dedicated for monitoring

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

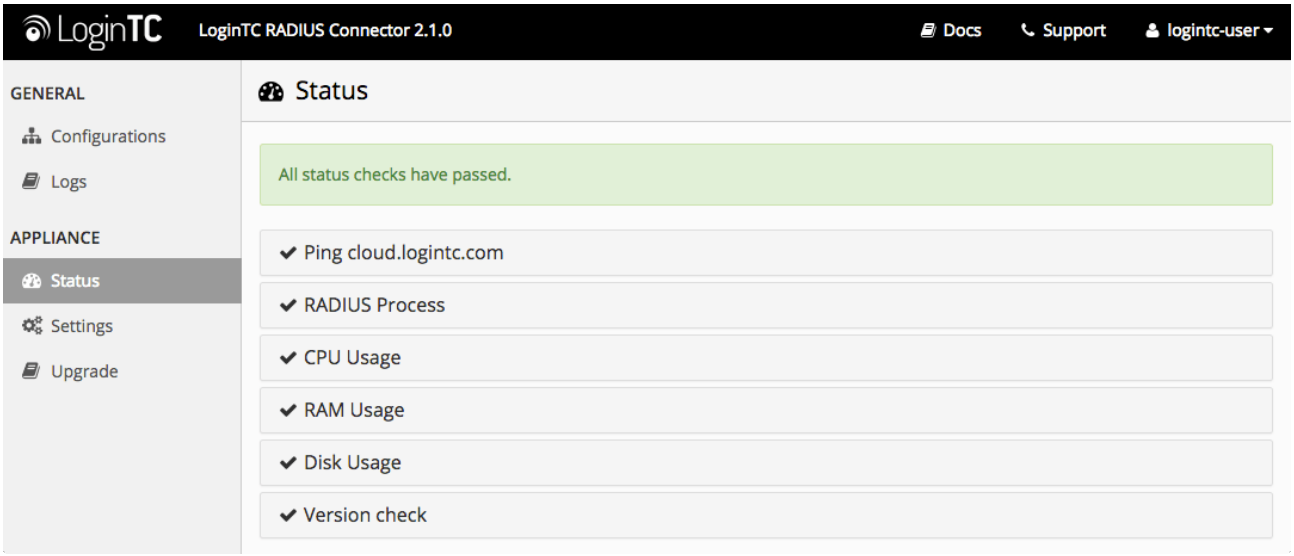
(Optional) Active Directory check for monitoring user

Recommend leveraging a dedicated service account for First Factor authentication.

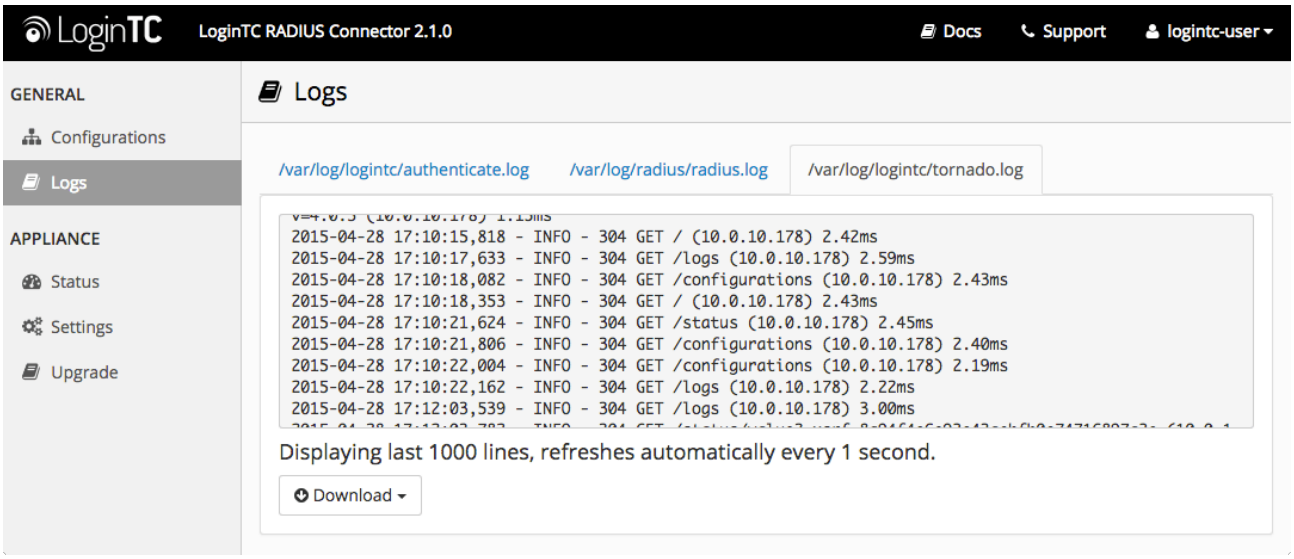
Troubleshooting

Not Authenticating

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



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



Email Support

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