

# Two factor authentication for OpenAM

---

 [sandbox-logintc.com/docs/connectors/openam.html](https://sandbox-logintc.com/docs/connectors/openam.html)

## Introduction

---

LoginTC OpenAM Connector allows administrators to incorporate two-factor authentication within their OpenAM authentication policies.

The following diagram illustrates a seamless LoginTC OpenAM Connector integration into an existing corporate network protected by OpenAM. The circled numbers indicate the step in a typical authentication flow.

---

The LoginTC OpenAM Authentication module is installed in your OpenAM server. It can be configured as a stand-alone policy or added to an existing authentication chain. When a user attempts to access a protected resource, the request is intercepted and the configured authentication policy is applied. When the LoginTC Authentication module is activated an out of band request is sent to the users mobile app. The request will launch the LoginTC app and gives the user an opportunity to approve or deny the request and then enter their PIN or passcode. The user's selection is sent back to module which will succeed in the OpenAM authentication chain if the credential was unlocked, otherwise the authentication will fail.

## Enterprise subscription required

---

Please contact our [sales team](#) for trial access to the LoginTC OpenAM Connector.

## Prerequisites

---

Before proceeding, please ensure you have the following:

- 1. LoginTC Cloud Administrator Account**

An administrator account allows you to perform management, maintenance and monitoring of your own LoginTC organization. An organization is where you manage domains, users, add and remove administrators and various other settings.

Sign Up for an administrator account at [LoginTC Admin](#).

- 2. OpenAM Installation**

If you do not already have OpenAM, full installation instructions can be found on ForgeRock's wiki: [OpenAM Installation](#). This installation guide was written for OpenAM 10.1.0.

- 3. User Data Store, e.g. Active Directory, LDAP Server, OpenDJ**

This datastore is the same as the one configured for your OpenAM server. Users from your data store will be synchronized with LoginTC Admin. Passwords are not stored in LoginTC Admin, only information about users like name, username and email.

## OpenAM Domain Creation

---

Protecting a corporate network or application is done by creating a new domain in your organization. There are various types of domains specific to what you are trying to protect. In this case, since the protected resource is controlled by OpenAM, use an OpenAM domain.

Steps to create a new OpenAM domain:

1. [Log in](#) to LoginTC Admin
2. Click **Domains**:
3. Click **Add Domain**:

Create Domain

4. Enter domain information:

Create Domain Form

### **Name**

Choose a name to identify your domain to you and your users

### **Connector**

OpenAM

## Installation

---

The LoginTC OpenAM Connector contains:

- OpenAM Authentication module
- OpenAM REST datastore client
- Java WAR utility to manage and sync data stores with LoginTC Admin

Before you begin, log into your OpenAM server via ssh:

1. Create a LoginTC directory:

```
mkdir -p /opt/logintc
cd /opt/logintc
```

2. Copy the latest LoginTC OpenAM Connector to /opt/logintc on your OpenAM server and unzip

```
unzip logintc-openam-connector-x.x.x.zip
```

## **Enterprise** subscription required

---

Please contact our [sales team](#) for trial access to the LoginTC OpenAM Connector.

## Configuration

---

### Run Install Script

---

Before you begin, log into your OpenAM server via ssh:

1. Go to LoginTC directory where the connector was downloaded

```
cd /opt/logintc
```

2. Stop your application server, i.e. tomcat

```
sudo service tomcat stop
```

3. Run install command

```
./install.sh /opt/logintc/logintcauth.jar /usr/share/tomcat/webapps/openam
```

First argument is the path to the `logintcauth.jar`  
Second argument is the path to the OpenAM exploded WAR

4. Start your application server, i.e. tomcat

```
sudo service tomcat start
```

### Enable Authentication Module

---

1. Navigate to your OpenAM installation, <http://www.myopenam.com:8080/openam>
- 

2. Log in using administrator credentials

3. Enable ssoadm, the configuration of core services:

1. Click on Configuration > Servers and Sites tab
  2. Click on your server under Servers
  3. Click on the Advanced tab
  4. Click the Add button and add a new entry: `ssoadm.disabled` with value `false`
  5. Save
- 

4. Restart your application server, i.e. tomcat

```
sudo service tomcat restart
```

5. Navigate to <http://www.myopenam.com:8080/openam/ssoadm.jsp>

6. Click create-svc
- 

7. Copy the contents from `/opt/logintc/amAuthLoginTCAuth.xml` and paste it in the form and click Submit
-

8. Navigate to `http://www.myopenam.com:8080/openam/ssoadm.jsp`

9. Click register-auth-module

10. Type in `com.cyphercor.logintc.openam.LoginTCAuth` and click Submit

11. Restart your application server, i.e. tomcat

```
sudo service tomcat restart
```

## Create New Module Instance

1. Navigate to your OpenAM installation, `http://www.myopenam.com:8080/openam`

2. Click Access Control

3. Select and click a Realm

4. Click Authentication tab

5. Create new Module Instance

1. Click New under Module Instances

2. Enter the name `LoginTC`

3. Select `LoginTC` as Type

4. Click OK

6. Click on `LoginTC` in the Modules list to configure the module

Property	Explanation
<code>Authentication Level</code>	The authentication level associated with this module
<code>Admin Host</code>	LoginTC Admin host
<code>Organization API Key</code>	The 64-character API key associated with your LoginTC Admin organization
<code>Domain ID</code>	The 40-character ID associated with your OpenAM domain
<code>Timeout</code>	Time in seconds to wait for authentication

7. When finished click Save

8. Restart tomcat on this server

```
sudo service tomcat restart
```

## User Management

---

One-way user synchronization of users from your OpenAM datastore directory to your OpenAM domain in LoginTC Admin is done by running `logintc-sync`.

`logintc-sync` will connect via REST to your OpenAM installation and sync users according to settings in `users.cfg` and fetch users from your directory using the `filter` query. If you wish to keep your user directory in sync with the users in your OpenAM domain in LoginTC Cloud, you may periodically run this command (without the `--dry-run` flag).

Go to conf in the installation directory:

```
cd /opt/logintc/conf
```

Copy the sample file as a template for your configuration file:

```
cp sample-users.cfg users.cfg
```

Open the file to modify its contents:

```
vi users.cfg

# openam
openam.protocol=http
openam.host=www.myopenam.com
openam.port=8080
openam.path=/openam
openam.admin.username=amadmin
openam.admin.password=password
openam.realm=/
openam.attr.username=uid
openam.attr.name=cn
openam.attr.email=mail
openam.filter.objectclass=person

# logintc
logintc.apikey=
logintc.domainid=
```

OpenAM configuration values:

Property	Explanation	Examples
<code>openam.protocol</code>	The protocol of your OpenAM server	http or https
<code>openam.host</code>	The host of your OpenAM server	www.myopenam.com
<code>openam.port</code>	The port of your OpenAM server	8080
<code>openam.path</code>	The path to your OpenAM installation	/openam
<code>openam.admin.username</code>	The username of a user with admin privileges in the realm	amadmin

Property	Explanation	Examples
<code>openam.admin.password</code>	The password of the above account	password
<code>openam.realm</code>	The realm in which the module is installed	/
<code>openam.attr.username</code>	The attribute containing the user's username	uid
<code>openam.attr.name</code>	The attribute containing the user's real name	cn
<code>openam.attr.email</code>	The attribute containing the user's email	mail
<code>openam.filter.objectclass</code> (optional)	The object class of the users	person

LoginTC configuration values:

Property	Explanation
<code>logintc.apikey</code>	The 64-character key associated with your LoginTC Admin organization.
<code>logintc.domainid</code>	The 40-character id associated with your OpenAM domain.

The API key is found on the LoginTC Admin [Settings](#) page. The Domain ID is found on your domain settings page.

Example:

```
$ cd /opt/logintc/bin
$ sudo ./logintc-sync /opt/logintc/conf/users.cfg
```

Output:

```
Processing /opt/logintc/users.cfg...
Querying OpenAM Rest service [http://www.myopenam.com:8080]
Found 2 users
+-----+-----+-----+-----+
| Realm | Username | Name      | Email                    |
+-----+-----+-----+-----+
| /     | john.doe | John Doe  | john.doe@example.com    |
| /     | jane.doe | Jane Doe  | jane.doe@example.com    |
+-----+-----+-----+-----+
Synchronizing 2 users...
Done.
```

Check that your users were added to your domain by viewing them in [LoginTC Admin](#).

There are several other options for managing your users within LoginTC:

## Testing

Once you have synchronized some users you can test the LoginTC module.

Navigate to `www.myopenam.com:8080/openam/UI/Login?module=LoginTC`

Enter the test user's username. You should now receive an authentication request on your mobile device. After authenticating you will be shown OpenAM user data.

---

## Authentication Chaining

---

Now that everything is tested you will want to create or modify an existing authentication chain to include the LoginTC.

1. Navigate to your OpenAM installation, <http://www.myopenam.com:8080/openam>
  2. Click Access Control
  3. Select and click a Realm
- 

4. Click Authentication tab
  5. Create new Authentication Chaining
    1. Click New under Authentication Chaining
    2. Enter `LoginTC` and click OK
- 
- 

6. Configure the new Authentication Chain

1. Click Add
  2. Selet LoginTC
  3. Set Criteria to `REQUIRED`
  4. Click Save
  5. Click Back to Authentication
- 
- 

7. Restart your application server, i.e. tomcat

```
sudo service tomcat restart
```

8. Test the new Authentication Chain

1. Navigate to [You can add other authentication modules to make chains. For example the following will first prompt for a username and password and then request a 2nd factor using the LoginTC:

---](http://www.myopenam.com:8080/openam/UI/Login?service>LoginTC</a></li><li>2. Enter the test user's username. You should now receive an authentication request on your mobile device. After authenticating you will be shown OpenAM user data.</li></ol><hr/></div><div data-bbox=)

Sample flow:

---

---

## User Enrolment

---

Once users have been synced to your OpenAM domain and you have tested your setup you can begin the process of user provisioning.

As seen in the [Testing Installation](#) section, users are issued a confirmation code which they use to load a new token on their mobile app. The Issue Token button will send an email to your user with full instructions on how to load a token. Sample email:

---

---