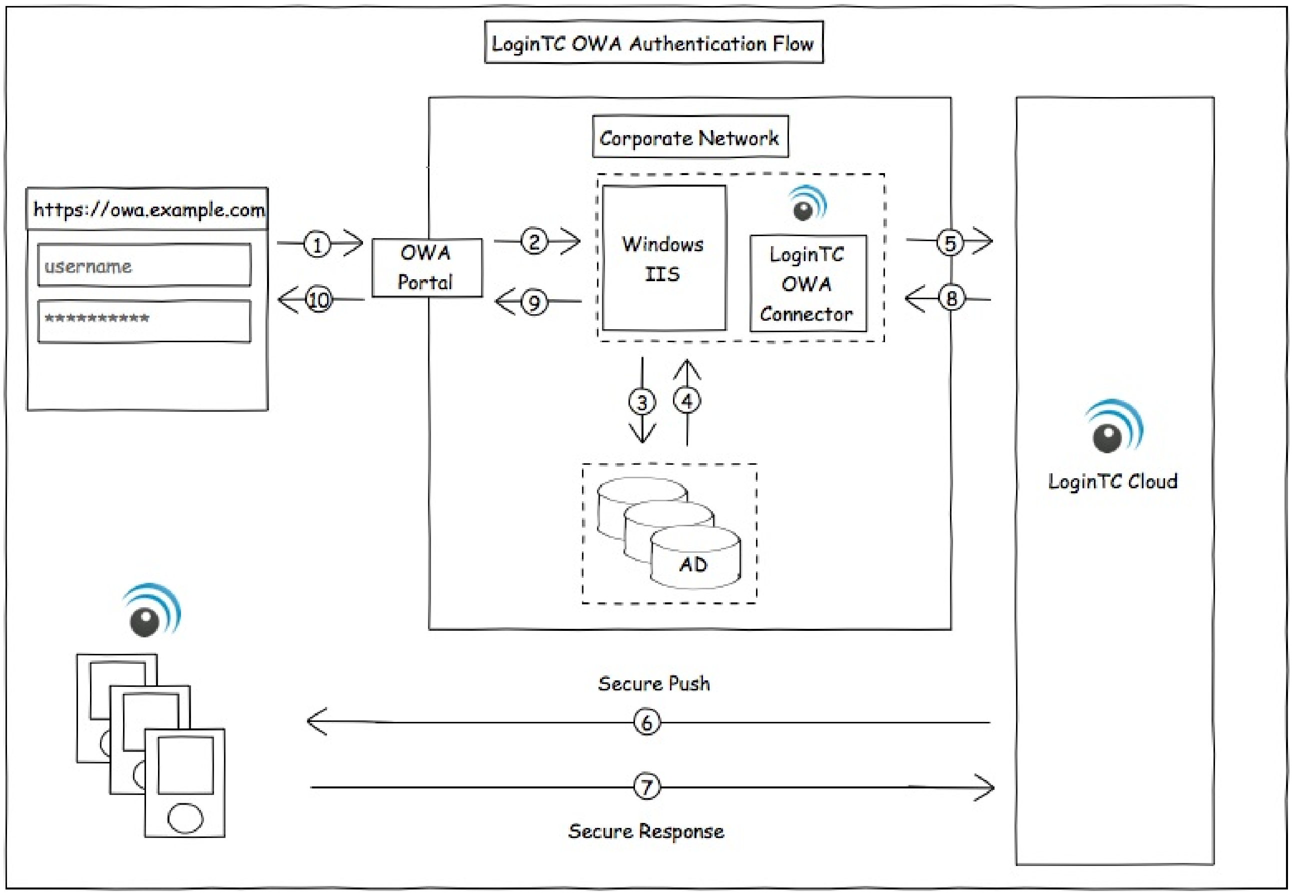
Two factor authentication for Microsoft Outlook Web App (OWA)

logintc.com/docs/connectors/owa.html

Overview

The LoginTC OWA Connector protects access to your Microsoft Outlook Web App by adding a second factor LoginTC challenge to existing username and password authentication.



Architecture and Authentication Flow

Subscription Requirement

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

User Experience

After entering the username and password into the Outlook Web App login, the user is shown a selection of second factor options. The user clicks a button to receive a LoginTC push notification, authenticates and is logged in.

Prerequisites

Before proceeding, please ensure you have the following:

- LoginTC Admin account
- Microsoft Windows Server 2012 R2 or Windows Server 2016
- Exchange 2013 or Exchange 2016
- .NET Framework 4.5.1 or higher

Working OWA Deployment

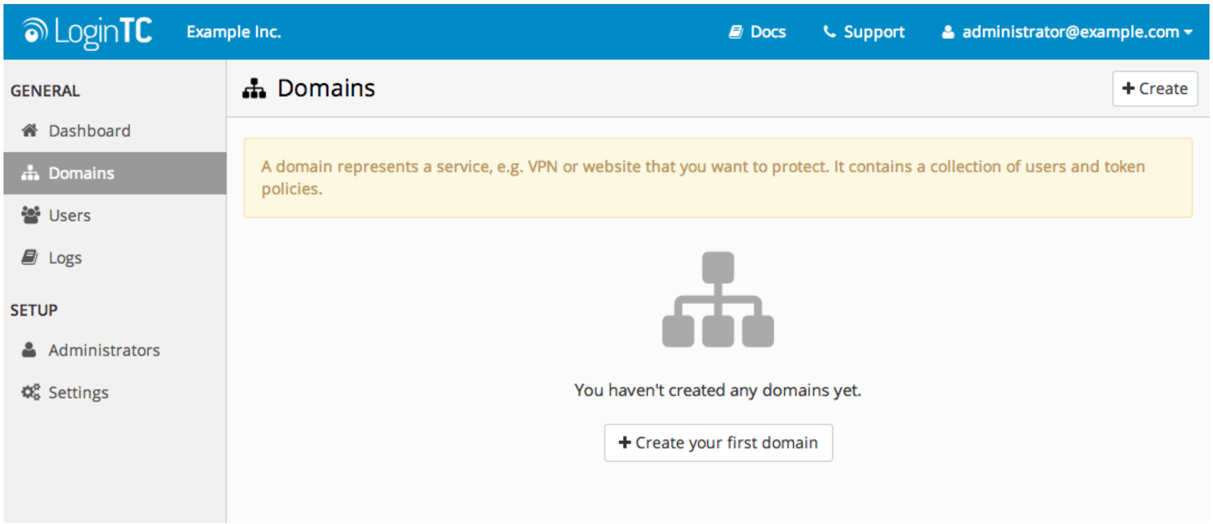
It is strongly recommended that you have a working and tested Outlook Web App deployment prior to adding LoginTC authentication.

LoginTC Domain Creation

Create a LoginTC domain in LoginTC Admin. The domain represents a service (e.g. your OWA) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

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

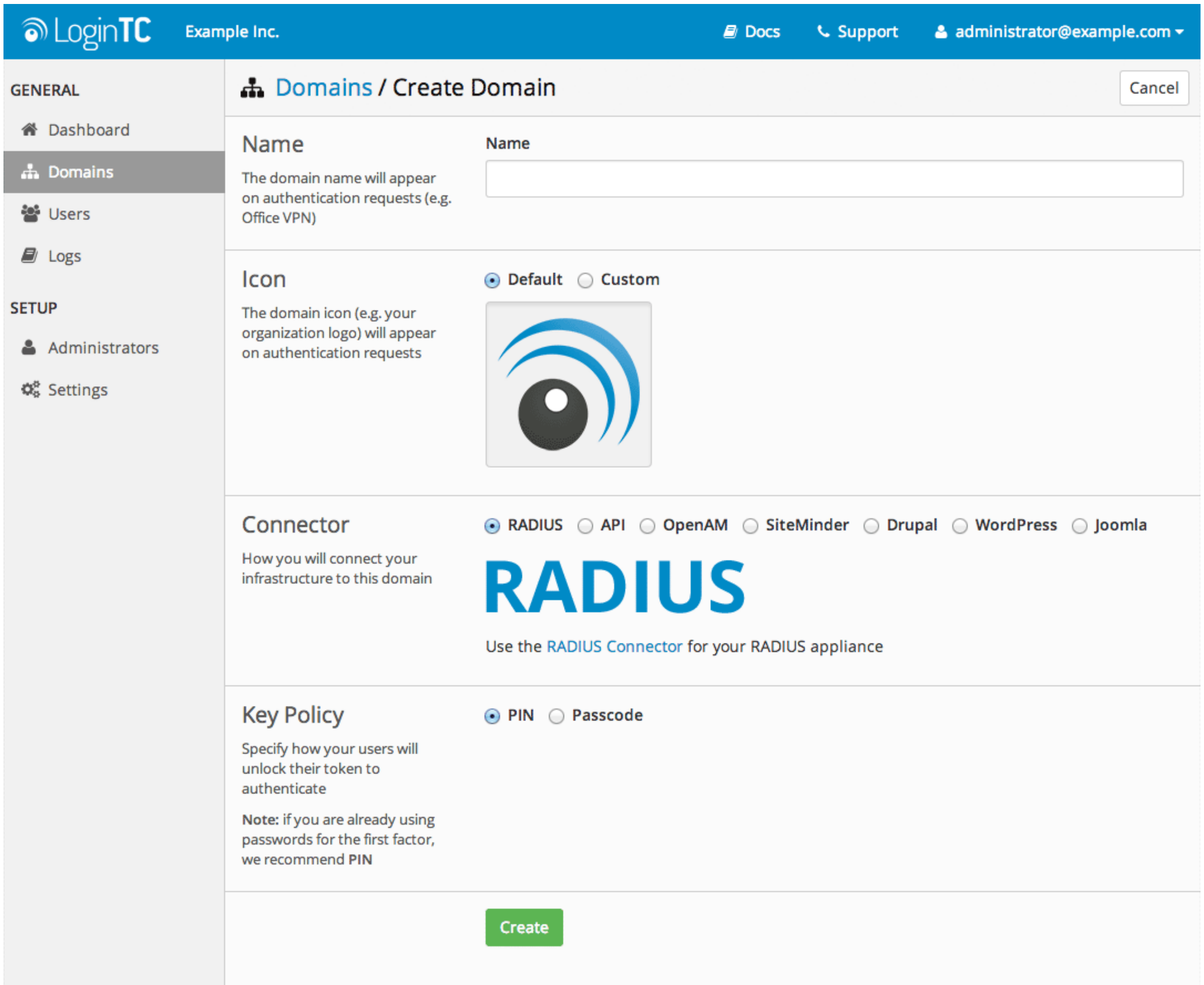
1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Create Domain**:



A domain represents a service, e.g. VPN or website that you want to protect. It contains a collection of users and token policies.

You haven't created any domains yet.

4. Enter domain information:



Domains / Create Domain

Name

The domain name will appear on authentication requests (e.g. Office VPN)

Name

Icon

The domain icon (e.g. your organization logo) will appear on authentication requests

● Default ○ Custom

Connector

How you will connect your infrastructure to this domain

● RADIUS ○ API ○ OpenAM ○ SiteMinder ○ Drupal ○ WordPress ○ Joomla

RADIUS

Use the RADIUS Connector for your RADIUS appliance

Key Policy

Specify how your users will unlock their token to authenticate

Note: if you are already using passwords for the first factor, we recommend **PIN**

● PIN ○ Passcode

Select the **API** option in the Connector section

Installation

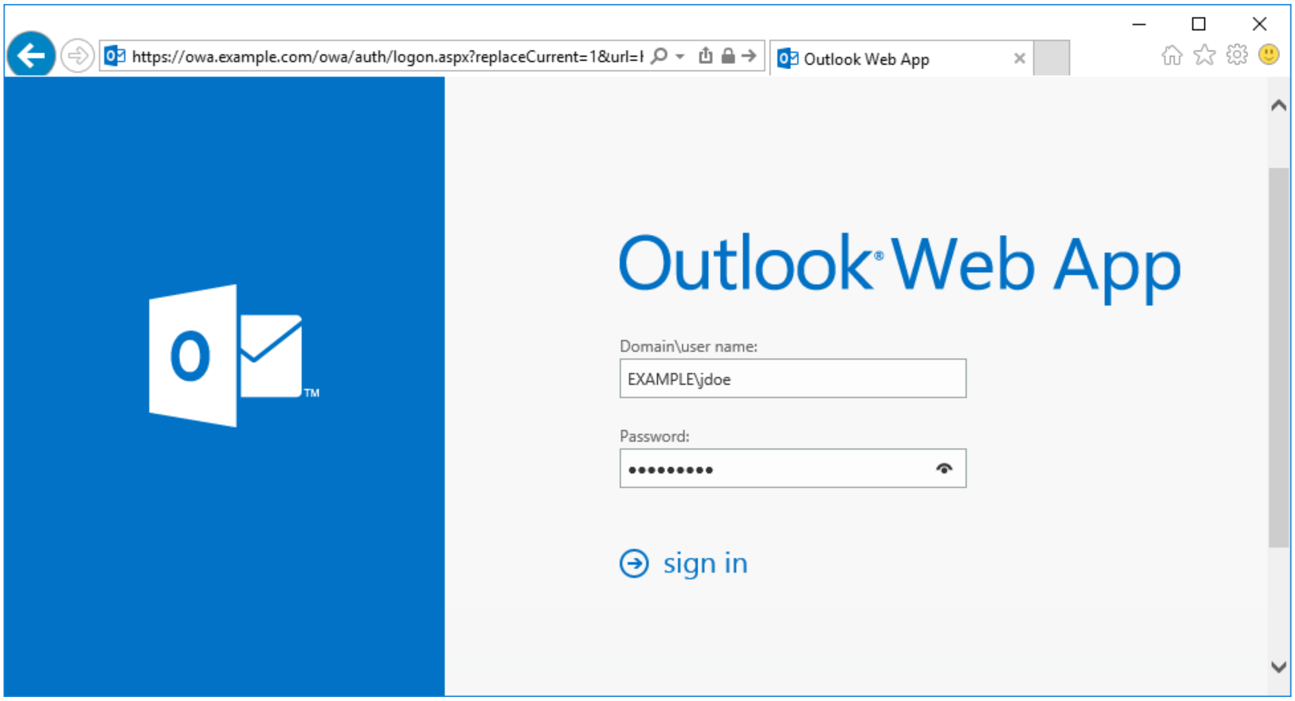
Follow the instructions to install the LoginTC OWA Connector:

The LoginTC OWA Connector is now installed and protecting your Outlook Web App.

Usage

This chapter demonstrates the possibilities of the LoginTC OWA Connector from both an administrator’s and end user’s point of view.

The OWA initial login page where the user enters their username and password is unmodified.

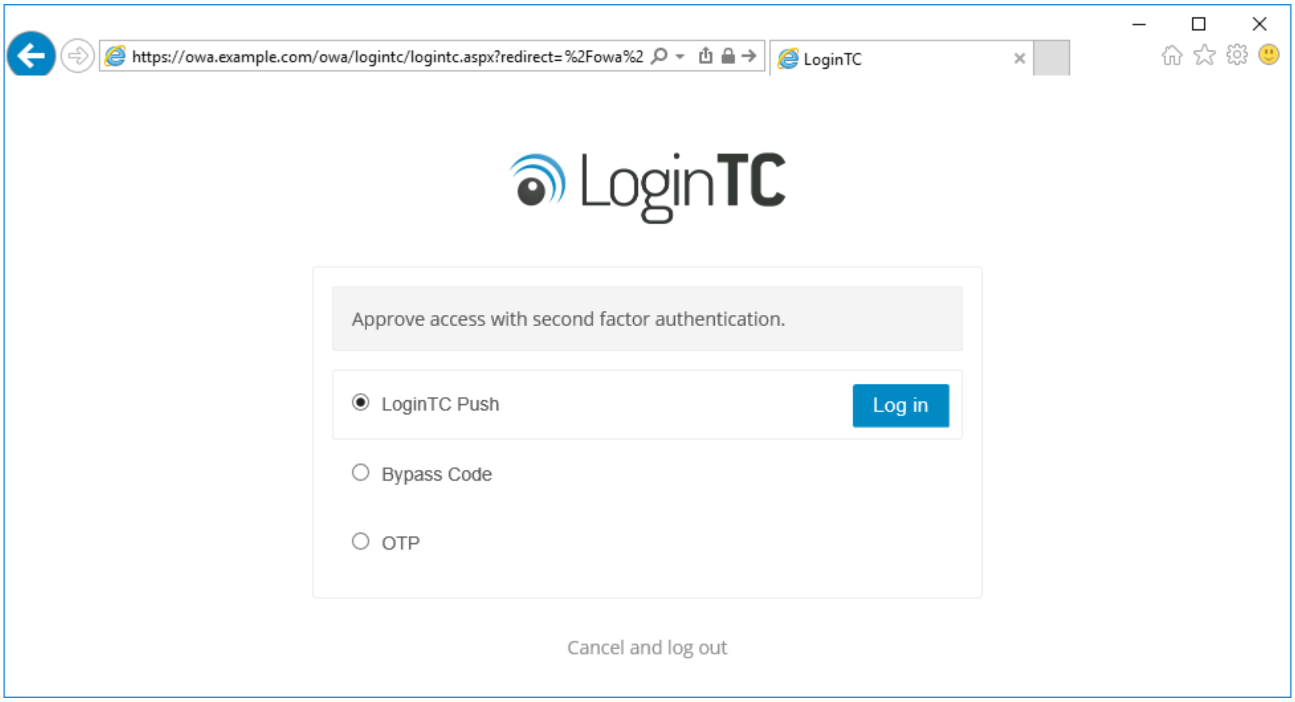

https://owa.example.com/owa/auth/logon.aspx?replaceCurrent=1&url=I
Outlook Web App
sign in

Outlook Web App

Domain\user name: EXAMPLE\jdoe

Password: ••••••••••

After successfully authenticating with their username and password, the user is presented with options to log in with LoginTC. The user may select to authenticate using LoginTC push, bypass codes, or OTPs.


https://owa.example.com/owa/logintc/logintc.aspx?redirect=%2Fowa%2
LoginTC
LoginTC
Log in
Cancel and log out

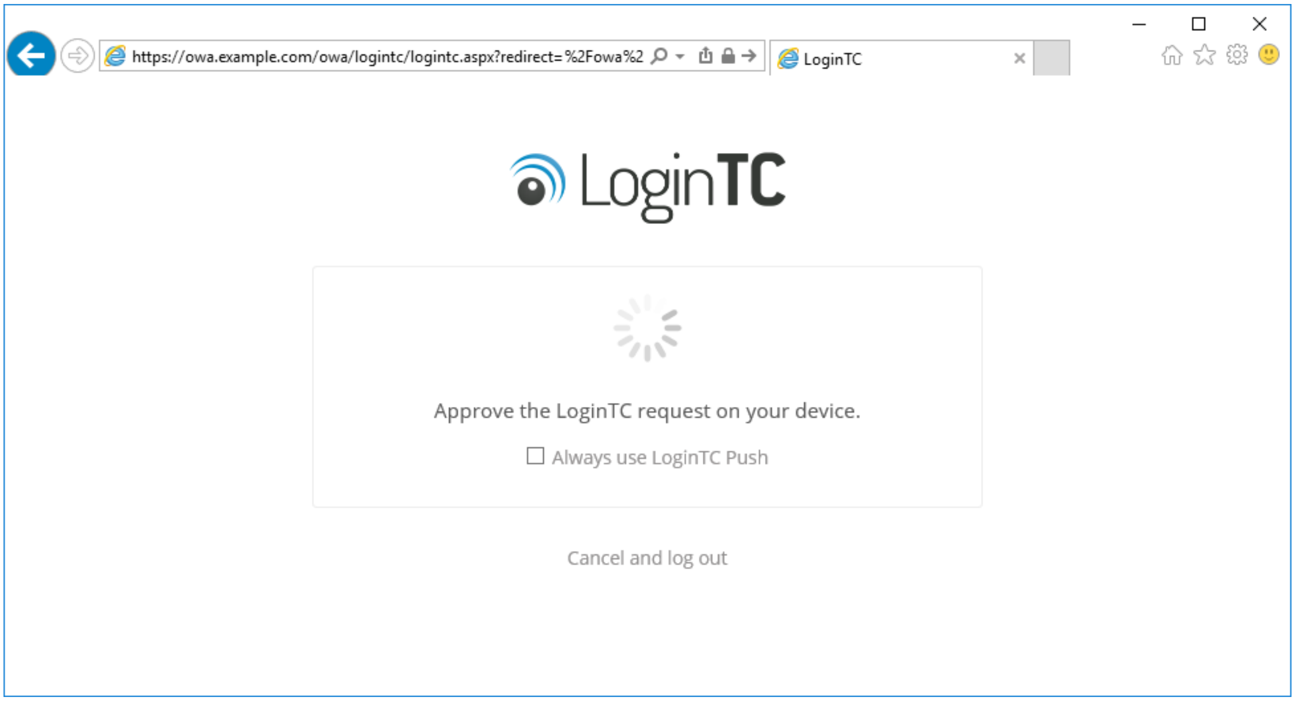
Approve access with second factor authentication.

● LoginTC Push

○ Bypass Code

○ OTP

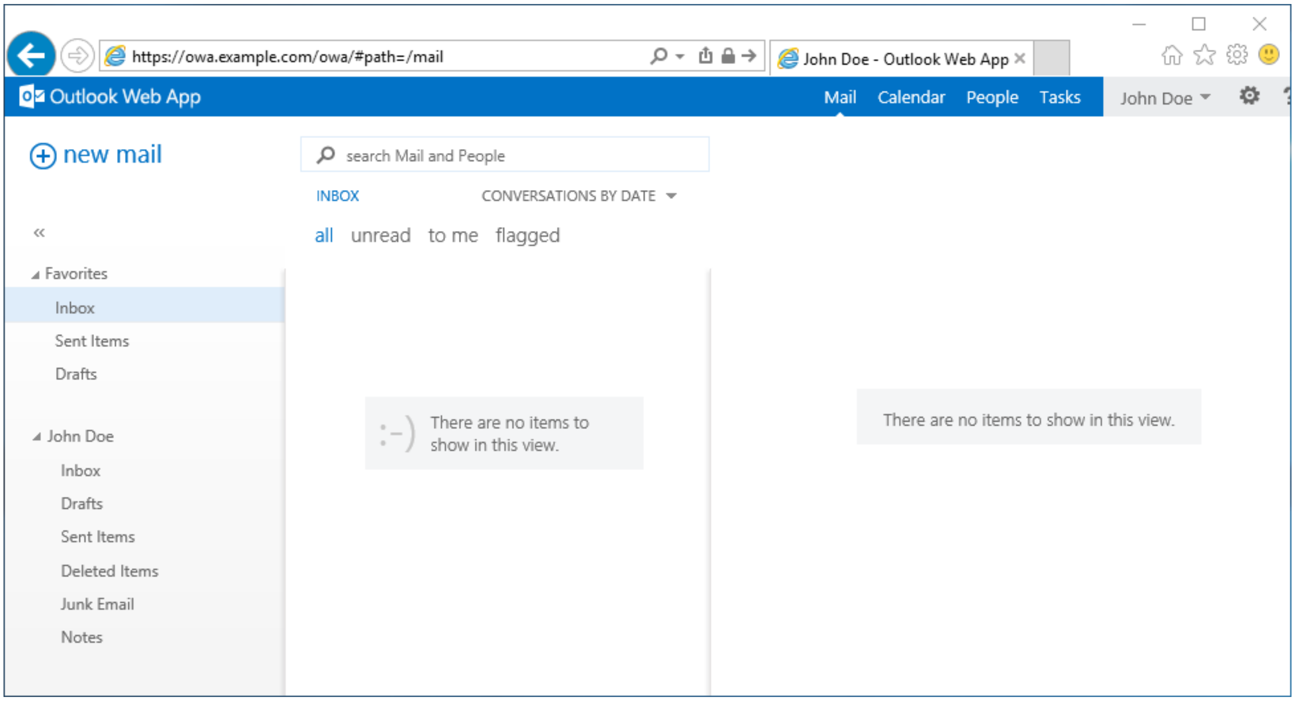
If the user selects LoginTC push, they are informed to approve the LoginTC requst on their device. The user is also presented with an option to remeber their LoginTC login choice. The next time the user logs in they will automatically receive a LoginTC push notification. The user may also cancel the login attempt and return to the login page.


https://owa.example.com/owa/logintc/logintc.aspx?redirect=%2Fowa%2

Approve the LoginTC request on your device.

□ Always use LoginTC Push

The user is brought to their OWA homepage after successfully authenticating with LoginTC.

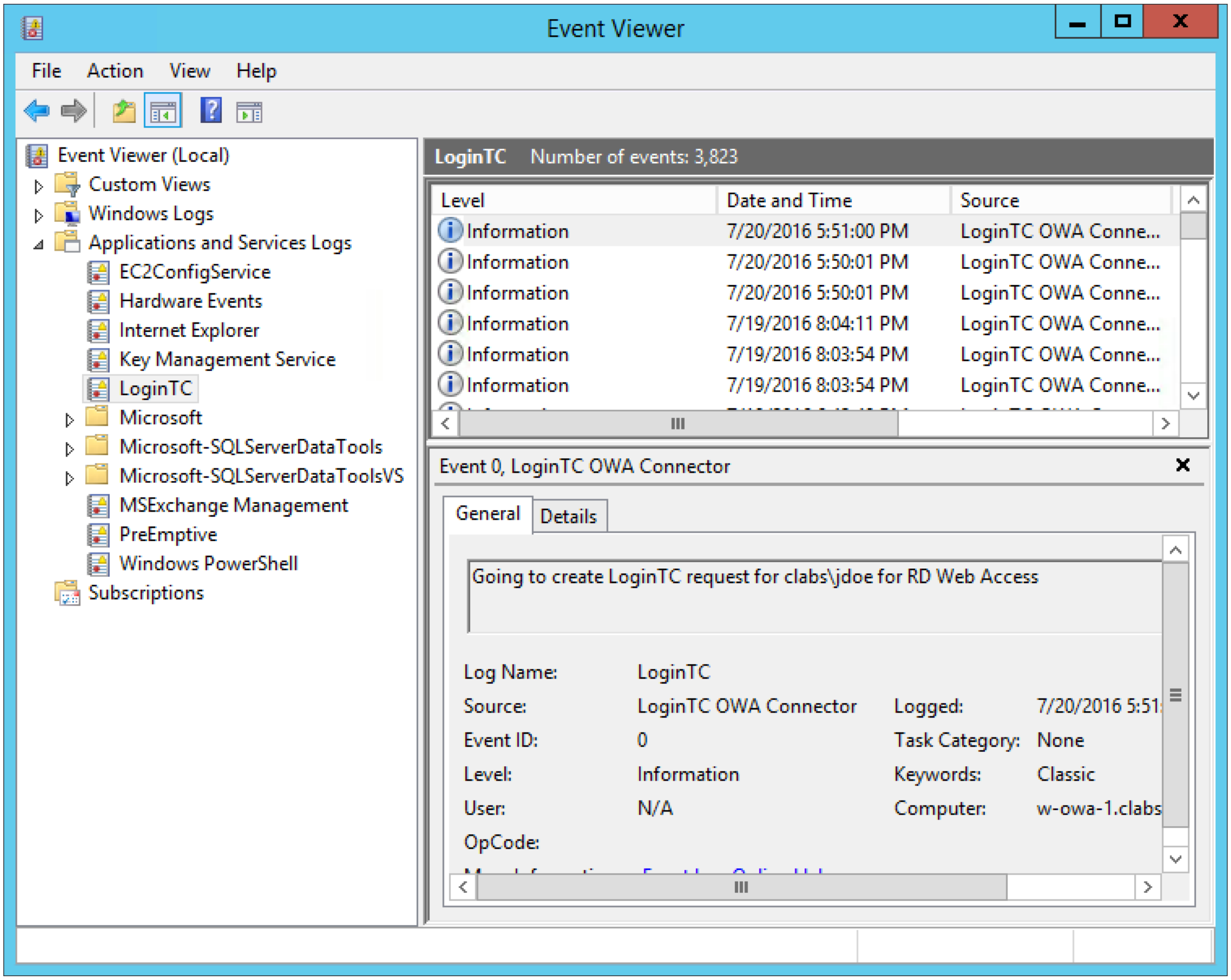

https://owa.example.com/owa/#path=/mail

:-) There are no items to show in this view.

There are no items to show in this view.

Logging

The LoginTC OWA Connector logs events to the Microsoft Event Viewer under **Applications and Service Logs** → **LoginTC**. LoginTC OWA Connector event logs are helpful in debugging issues.



LoginTC Number of events: 3,823

Level	Date and Time	Source
Information	7/20/2016 5:51:00 PM	LoginTC OWA Conne...
Information	7/20/2016 5:50:01 PM	LoginTC OWA Conne...
Information	7/20/2016 5:50:01 PM	LoginTC OWA Conne...
Information	7/19/2016 8:04:11 PM	LoginTC OWA Conne...
Information	7/19/2016 8:03:54 PM	LoginTC OWA Conne...
Information	7/19/2016 8:03:54 PM	LoginTC OWA Conne...

Event 0, LoginTC OWA Connector

Going to create LoginTC request for clabs\jdoe for RD Web Access

Log Name:	LoginTC		
Source:	LoginTC OWA Connector	Logged:	7/20/2016 5:51:
Event ID:	0	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	w-owa-1.clabs
OpCode:			

Passthrough

Passthrough allows you to specify which set of users should be challenged with LoginTC second-factor authentication, and which ones will not. This is often useful when testing and when rollying out a deployment to minimize the impact on others.

Static User List

Setting a static user list tells the LoginTC OWA Connector which users must be challenged for LoginTC second-factor authentication. All other users will be passed through without requiring a second-factor authentication.

Instructions to set a static list of users to be challenged:

1. Navigate to `C:\Program Files\Cyphercor\LoginTC OWA Connector`.
2. Create a new file `users.txt` in Notepad.
3. Populate the file with a list of users, one line at a time, in the following format: `DOMAIN\username`
4. Save the file.
5. Your change will be picked up by the connector within 60 seconds.

If the `users.txt` file does not exist then all users will be challenged with LoginTC second-factor authentication.

Group List

Setting a group list tells the LoginTC OWA Connector which AD security group members must be challenged for LoginTC second-factor authentication. All other users not belonging to any of the listed AD security groups will be passed through without requiring a second-factor authentication.

Instructions to set a list of AD security groups to be challenged:

1. Navigate to `C:\Program Files\Cyphercor\LoginTC OWA Connector`.
2. Create a new file `groups.txt` in Notepad.
3. Populate the file with a list of AD security groups, one line at a time.
4. Save the file.
5. Your change will be picked up by the connector within 60 seconds.

If the `groups.txt` file does not exist then all users will be challenged with LoginTC second-factor authentication (unless a static user list file exists).

Email Support

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