Duo - Mimecast

.

Introduction

As business applications move from on-premises to cloud hosted solutions, users experience password fatigue due to disparate logons for different applications. Single sign-on (SSO) technologies seek to unify identities across systems and reduce the number of different credentials a user has to remember or input to gain access to resources.

While SSO is convenient for users, it presents new security challenges. If a user's primary password is compromised, attackers may be able to gain access to multiple resources. In addition, as sensitive information makes its way to cloud-hosted services it is even more important to secure access by implementing two-factor authentication.

Duo is able to integrate with Mimecast to protect access to the Mimecast Personal Portal, Admin Portal and End users apps including Mimecast Mobile app on iOS and Android

Duo Access Gateway

Duo Access Gateway (DAG), our on-premises SSO product, layers Duo's strong authentication and flexible policy engine on top of Mimecast logins using the Security Assertion Markup Language (SAML) 2.0 authentication standard. Duo Access Gateway authenticates your users using existing Active Directory credentials and prompts for two-factor authentication before permitting access to Mimecast.

Duo Access Gateway is part of the Duo Beyond and Duo Access plans, so you can define policies that enforce unique controls for each individual SSO application. For example, you can require that Mimecast users complete two-factor authentication at every login, but only once every seven days when accessing Google Apps. Duo checks the user, device, and network against an application's policy before allowing access to the application.

Deploy Duo Access Gateway

Install Duo Access Gateway on a server in your DMZ. Follow our instructions for deploying the server, configuring DAG settings, and adding your primary authentication source.

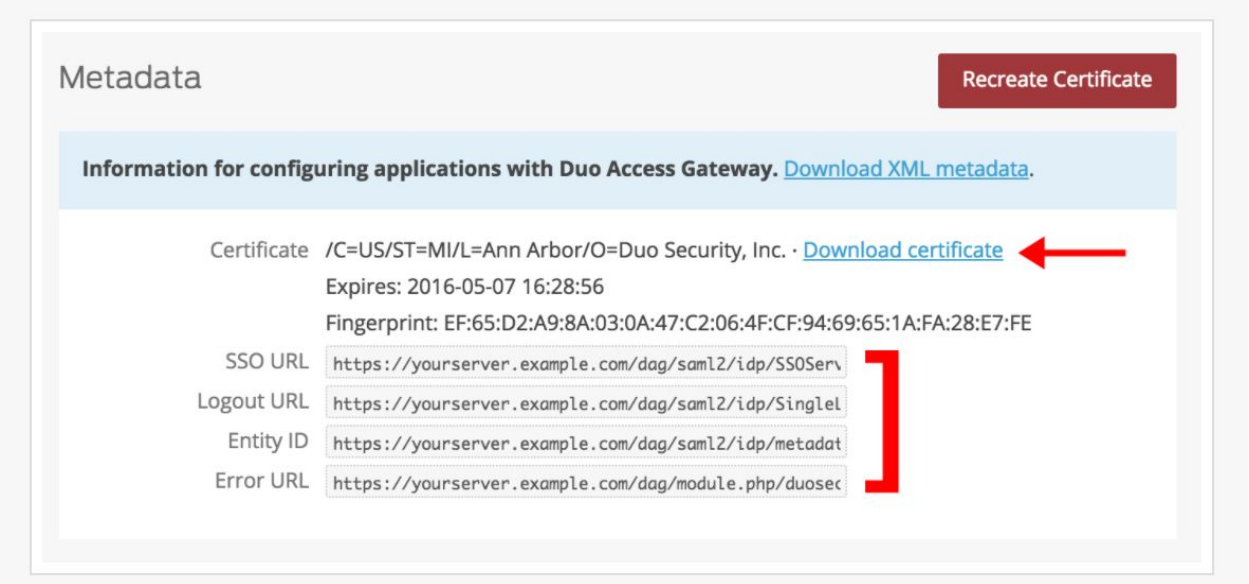
Add the attributes from the table below that correspond to the Duo attributes Mail attribute and Username attribute in the "Attributes" field when configuring your Active Directory or OpenLDAP authentication source in the DAG admin console, separated by a comma. For example, if Active Directory is your authentication source, enter mail,sAMAccountName in the "Attributes" field.

Duo Attribute	Active Directory	OpenLDAP
Mail attribute	mail	mail
Username attribute	sAMAccountName	uid

If your organization uses other directory attributes than the ones listed here then enter those attribute names instead. If you've already configured the attributes list for another cloud service provider, append the additional attributes not already present to the list, separated by a comma.

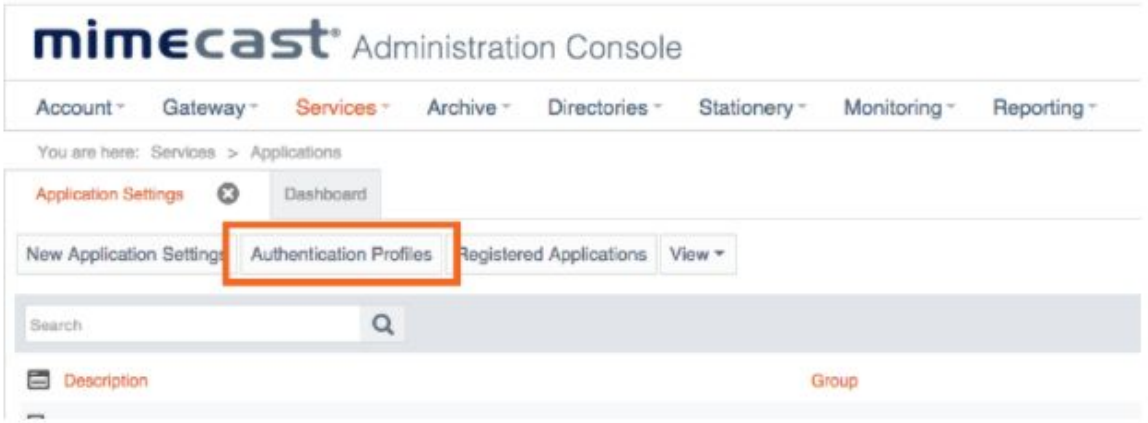
After completing the initial DAG configuration steps, click Applications on the left side of the Duo Access Gateway admin console.

Scroll down the Applications page to the Metadata section. This is the information you need to provide to Mimecast when configuring SSO. Click the Download Certificate link to obtain the token signing certificate (the downloaded file is named "dag.crt").

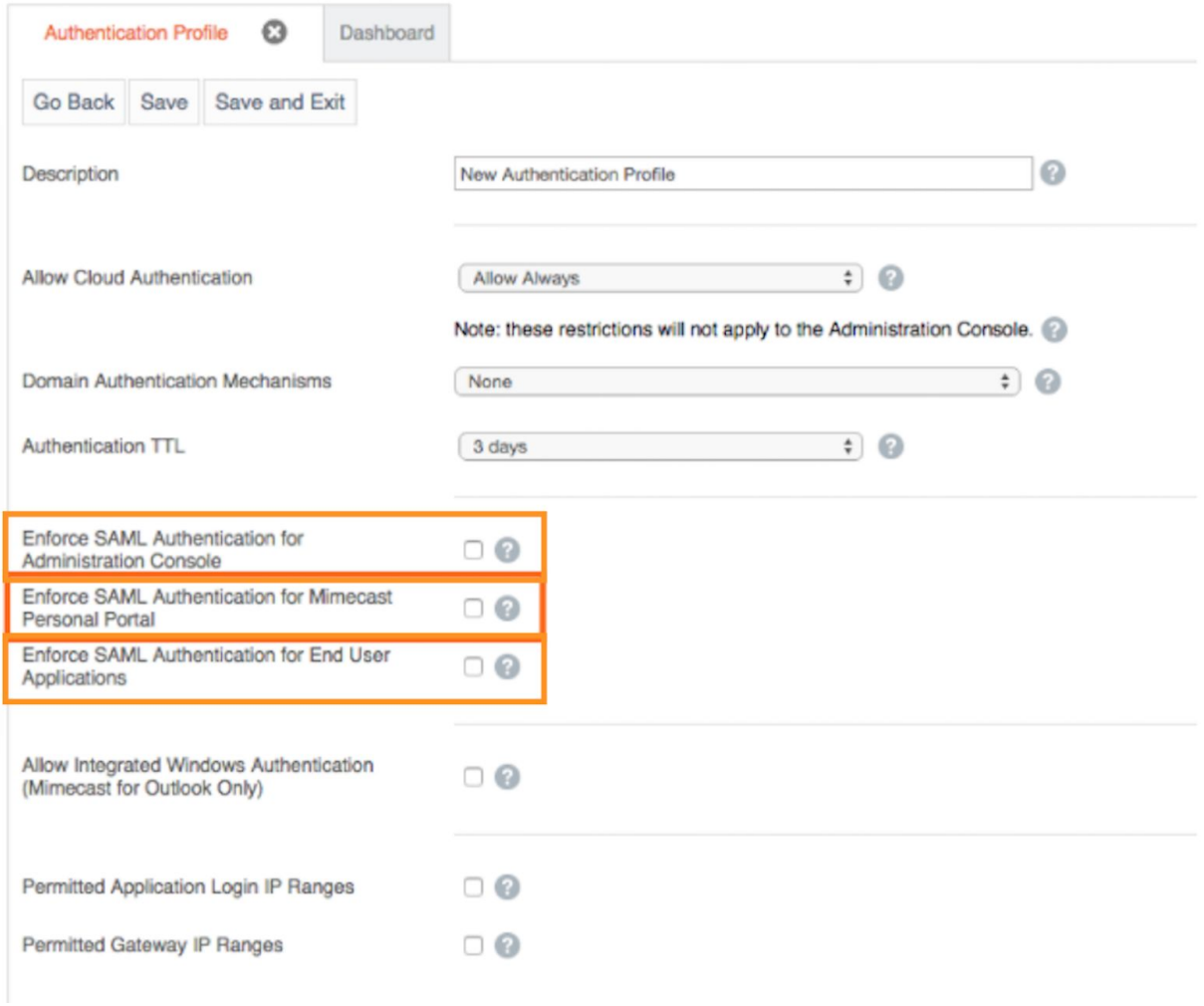


Enable SSO in Mimecast (Mimecast Personal Portal / End User Applications)

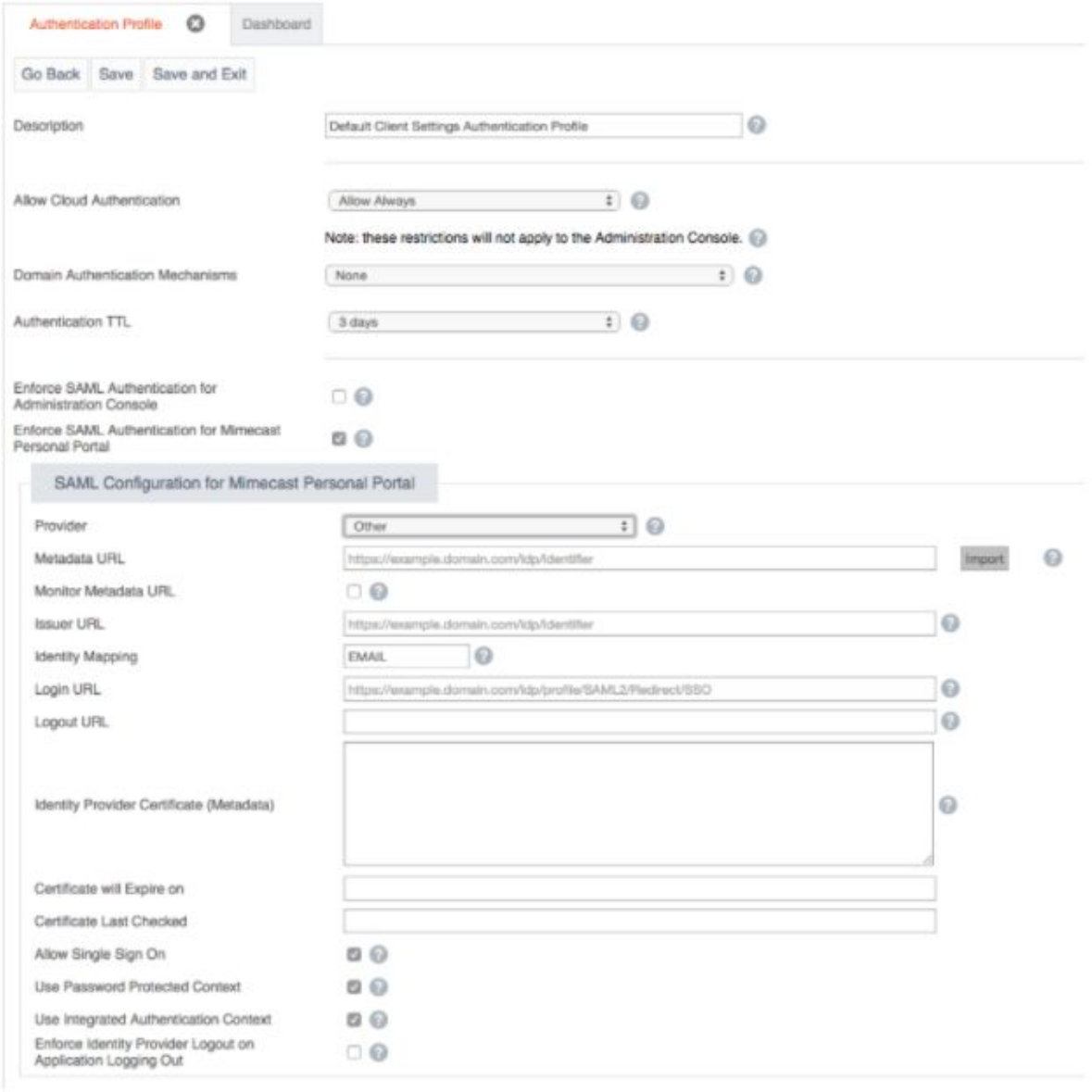
Login to the Administration Console.
Navigate to the Administration | Services | Applications menu.
Select the Authentication Profiles button.



Select an existing Authentication Profile to update or select the New Authentication Profile button to create a new one (creating a new Auth Profile with just the users you want to test with is useful if trialling Duo) .
Enter a Description for the new profile.
Select Enforce SAML Authentication for Mimecast Personal Portal, End User Applications and / or Admin Console.



The screen expands to reveal the SAML Settings:



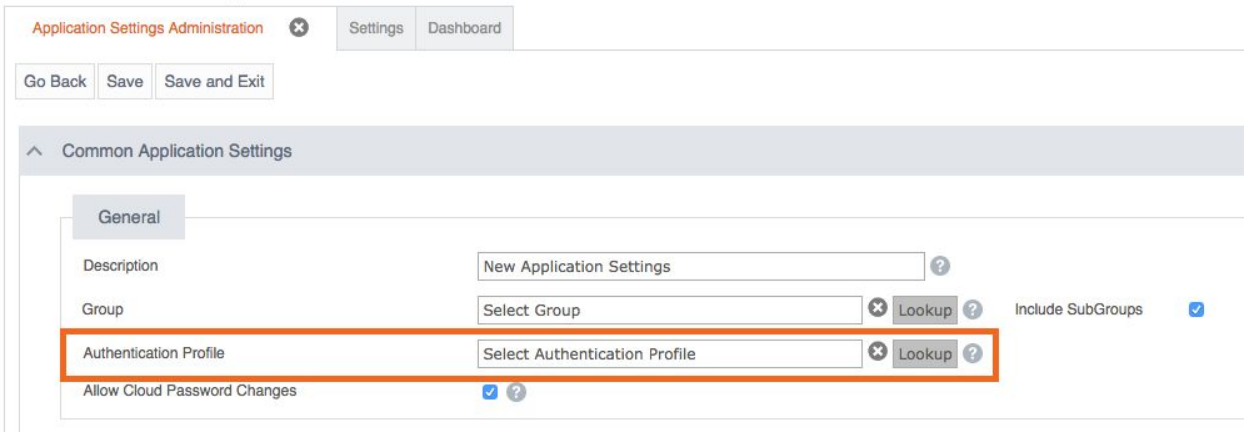
Select Other as your Identity Provider from the Provider drop down list.

Copy and paste your Entity ID from the Duo Access Gateway in the Metadata URL field and Select Import.

Choose to *Allow Single Sign On*. This setting enables / disables Identity Provider Initiated Sign On.

Once your Authentication Profile is complete, you need to reference it in an Application Setting in order for it to be applied. To do this:

Log in to the Administration Console.
Navigate to the Administration | Services | Applications menu
Select the Application Setting that you want to use.
Use the Lookup button to find the Authentication Profile you want to reference.
Click on the Select link on the lookup page.



Select Save and Exit to apply the change.

Create the Mimecast Application in Duo (Personal Portal / End User Applications)

Log on to the Duo Admin Panel and navigate to Applications.

Click Protect an Application, locate SAML - Service Provider in the applications list, and click Protect this Application. See Getting Started for help

Enter your Mimecast Entity ID

The EntityID value will be different depending on the Mimecast grid that your organization's Mimecast account is hosted. Below are the expected values for each grid:

- Europe - eu-api.Mimecast.com.ACCOUNTCODE
- United States - us-api.Mimecast.com.ACCOUNTCODE
- South Africa - za-api.Mimecast.com.ACCOUNTCODE
- Australia - au-api.Mimecast.com.ACCOUNTCODE
- Offshore - jer-api.Mimecast.com.ACCOUNTCODE

  Where ACCOUNTCODE is your unique Mimecast account code as specified in the Admimistration |

Account | Account Settings page of the Administration Console.

Enter your Assertion Consumer Service URL

The Assertion Consumer Service URL will also be different depending on the Mimecast grid that your organization's Mimecast account is hosted. Below are the expected values for each grid:

- Europe - https://eu-api.Mimecast.com/login/sso/mpp
- Untied States - https://us-api.Mimecast.com/login/sso/mpp
- South Africa - https://za-api.Mimecast.com/login/sso/mpp
- Australia - https://au-api.Mimecast.com/login/sso/mpp
- Offshore - https://jer-api.Mimecast.com/login/sso/mpp

Example Config

You can adjust additional settings for your new SAML application at this time — like changing the application's name from the default value, enabling self-service, or assigning a group policy — or come back and change the application's policies and settings after you finish SSO setup. If you do update any settings, click the Save Changes button when done.

Click the Download your configuration file link to obtain the Mimecast application settings (as a JSON file).

Add the Mimecast Application to Duo Access Gateway

Return to the Applications page of the DAG admin console session.

Click the Choose File button in the "Add Application" section of the page and locate the Mimecast SAML application JSON file you downloaded from the Duo Admin Panel earlier. Click the Upload button after selecting the JSON configuration file.

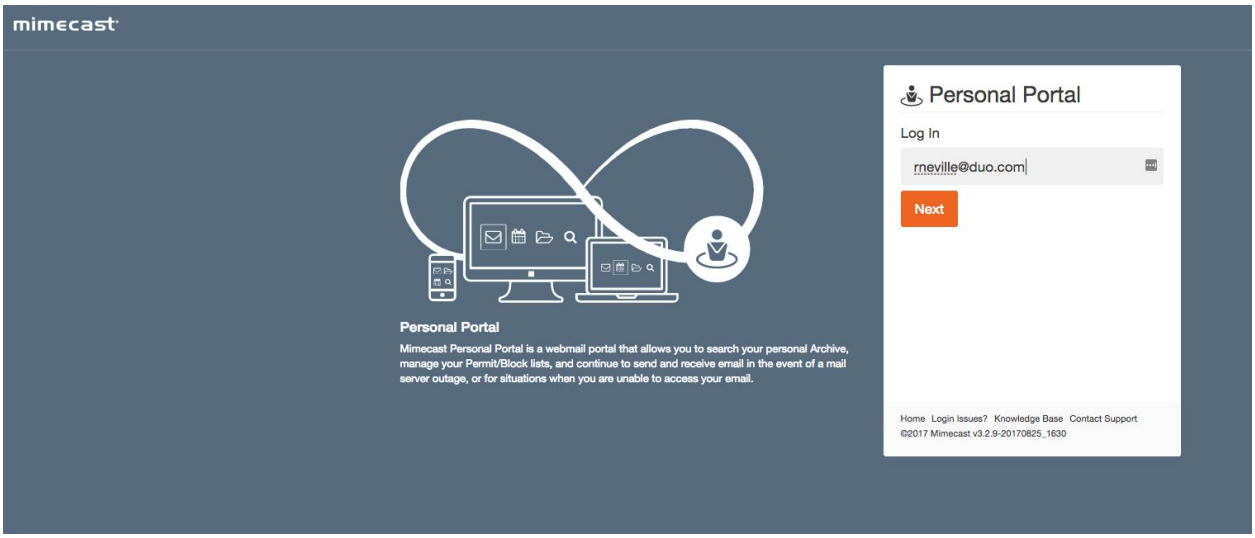
The Mimecast SAML application is added.

Verify SSO

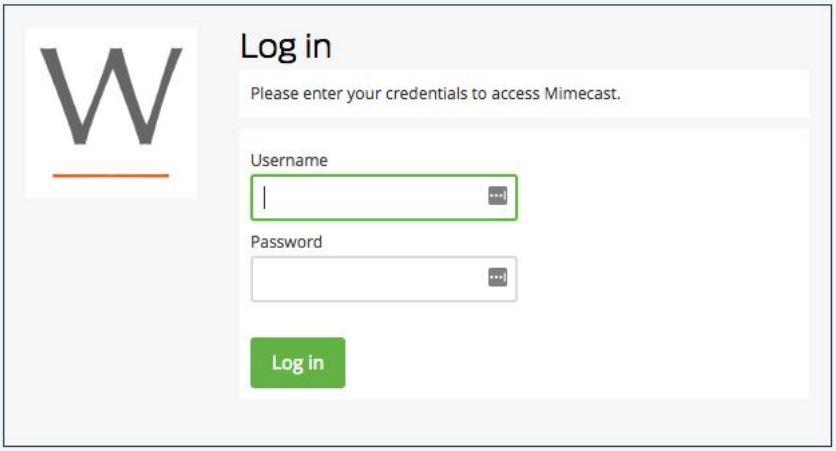
When using service provider initiated SAML authentication, your users must access the Mimecast Personal Portal using the regional URL.

E.g. https://login-uk.Mimecast.com

Enter Username



Redirected to DAG for Authentication


Log in
Please enter your credentials to access Mimecast.
Username
Password
Log in