

Sentry SSO with Mimecast

Contents

- [1 Setup AuthControl Sentry Keys](#)
- [2 Setup SSO on Mimecast](#)
- [3 Configure Check Password with Repository on the Swivel Core](#)
- [4 Setup AuthControl Sentry Application definition](#)
- [5 Setup AuthControl Sentry Authentication definition](#)
- [6 Testing authentication to Mimecast via Swivel AuthControl Sentry](#)
- [7 Troubleshooting](#)

Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on Mimecast.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

Setup SSO on Mimecast

To configure SSO setting on your Mimecast accounts you have to access your Admin console by simply going to <https://console-uk-2.mimecast.com/mimecast/admin> You should see an Admin console with an option "Services" similar to the one below:

Service Notifications

All Mimecast services are operating normally. No recent service interruptions to report.

Product News

We are excited to announce global availability of the first phase of the updated Administration Console. If you aren't already, start using it today to benefit from the great new navigation and features. The location and guidance notes have been published on Mimecast Central

Activity Over 24 hrs

Held Email

n/a

Rejected Email

n/a

Bounced Email

n/a

Attachments Linked

n/a

Attachments Blocked

n/a

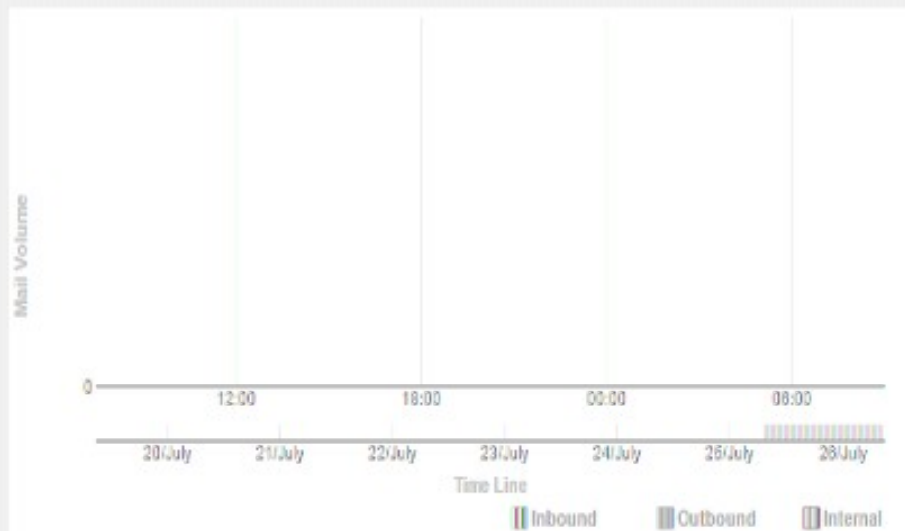
Policy Edits

n/a

Last refreshed at 09:17 AM



Total Email Traffic



Directory Connectors

Service Not Configured

Last refreshed at 09:35 AM

Journal Connectors

n/a

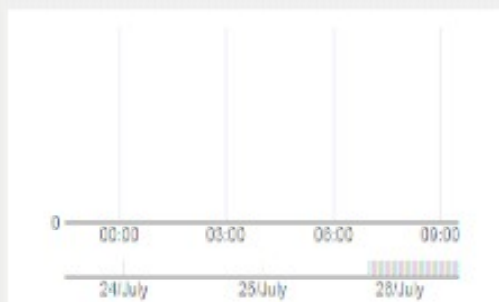
Last refreshed at 09:35 AM

Exchange Services

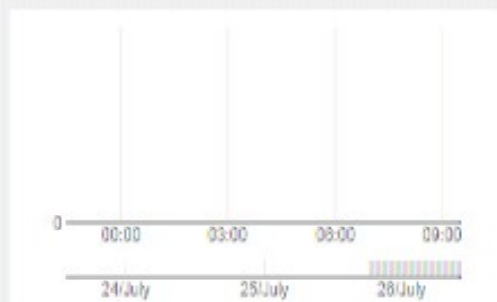
n/a

Last refreshed at 09:35 AM

Inbound Email Queue



Outbound Email Queue



Rejections

Open Relay Not Allowed

Recipient Address

Attempt Redirected to Primary MX

Administrative Lockout

Message Body Rejection

Last refreshed at 09:27 AM

Login Information

Account Name

Swivel Secure

Logged In Since

2016-07-26 09:21:49

Security Passphrase

Account Code

C75A125

Support Code

9BE6

When you click on the Services you will be shown different profiles. You have to click on the button "Authentication Profiles" and select the User group for which to use SSO. For this example we are using "Swivel Users".

mimecast® Administration Console

Account

Services

You are here: Services > Applications

Application Settings

Dashboard

New Application Settings

Authentication Profiles

View

Search

Description	Group	Authentication
Default Application Settings	All_Group_Users	Default Authentication
Swivel Users	Swivel Users	Swivel Users

Build: 3.0.56.7-R0711 Version: 3.0.56.7

After clicking on the authentication profile you will have to fill in the details for your AuthControl Sentry such as:

Set the Login, Logout URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Sign-in page URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint*

Sign-out page URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout*

Now navigate to your AuthControl Sentry metadata page as below(*https://<FQDN_OF_SENTRY_SERVER>/sentry/metadata/generatedMetadata.xml*) and copy the content of this page.

mimecast® Administration Console

Account ▾ Services ▾

You are here: Services > Applications

Authentication Profile ✕

Dashboard

Go Back

Save

Save and Exit

Description

Swivel Users

Allow Cloud Authentication

Allow Always

Domain Authentication Mechanisms

None

2-Step Authentication

None

Authentication TTL

3 days

Enforce SAML Authentication for
Administration Console



Enforce SAML Authentication for Mimecast
Personal Portal



SAML Configuration for Mimecast Personal Portal

Provider

Other

Metadata URL

Monitor Metadata URL



Issuer URL

https://192.168.11.114:8085/sentry/saml20endpoint

Identity Mapping

EMAIL

Login URL

https://192.168.11.114:8085/sentry/saml20endpoint

Logout URL

https://192.168.11.114:8085/sentry/singlelogout

Identity Provider Certificate (Metadata)

MIIFVzCCBP2gAwIBAgIJAks92WUrKu1yMA8GCMGSAFlAwQDAjCBjzELMAkGA1UEBhMCR0IxETAQBgNVBAgMCV1vcmtzaGlyZTERMA8GA1UEBwwIV2V0aGVyYnkxDzANBgNVBAoMB1N3aXZlbDEMAoGAA1UECwwDRGV2MQ8wDQYDVQQDDAZTZW50cnkxKTANBgkqhkiG9w0BCQEWGmwubW9yYXxlc0Bzd212ZWxzZW50cmUuY29tMB4XDTE2MDcvNTEzNTM0M1oXDTE2MDgvNDEzNTM0M1owY8xC

Certificate will Expire on

2016-08-24 14:53

Certificate Last Checked

Allow Single Sign On



Use Password Protected Context



Use Integrated Authentication Context



Enforce Identity Provider Logout on
Application Logging Out



Enforce SAML Authentication for End User
Applications



Import

Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

Setup AuthControl Sentry Application definition

Please note: you must have setup a Mimecast SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Mimecast, click the Add Application button and select SAML - Mimecast.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS is SAML (Security Assertion Markup Language) n

Name

Mimecast

Image

Mimecast.png

Points

100

Portal URL

https://login-uk.mimecast.c

Endpoint URL

Entity ID

eu-api.mimecast.com.C75A

Federated Id

givenname

Name: Mimecast

Image: Mimecast.png(selected by default)

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: (this Portal URL is Mimecast login URL which you can usually access on: <https://login-uk.mimecast.com/m/portal/login> note for different countries it might be a different URL)

Entity URL: N/A

Entity ID: eu-api.mimecast.com.ACCOUNT_NUMBER (Entity ID is a eu-api.mimecast.com. with an Account number such: eu-api.mimecast.com.C75A125)

Federated id: email

Account Number can be found on the Mimecast Admin Console [at the bottom left corner](#)

Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Mimecast authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Mimecast Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

Testing authentication to Mimecast via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. **<https://login-uk.mimecast.com/logon>**

Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. **<https://mycompanysentrydomain/sentry/startPage>** On a Start Page you will be able to see a new Mimecast Icon on which you can click and proceed with authentication (as you would by going straight to the mimecast page)

Please select an application

The Mimecast logo, consisting of the word 'mimecast' in a lowercase, sans-serif font.The Juniper Networks logo, with 'JUNIPER' in a large, thin, uppercase font and 'NETWORKS' in a smaller, thin, uppercase font below it.The ServiceNow logo, with 'servicenow' in a lowercase, sans-serif font, where the 'now' part is in red.

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.



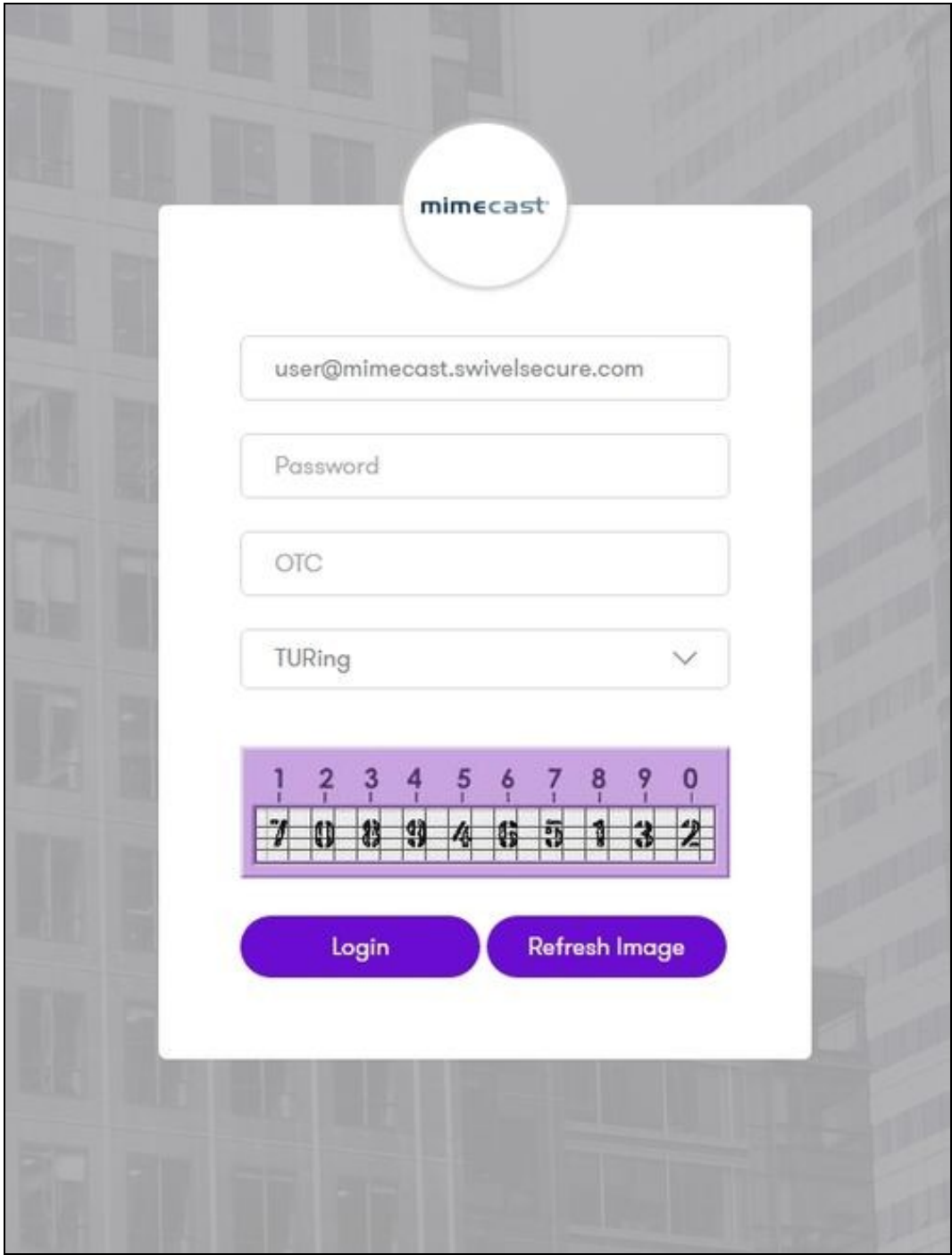
Personal Portal

Mimecast Personal Portal is a webmail portal that allows you to search your personal Archive, manage your PermitBlock lists, and continue to send and receive email in the event of a mail server outage, or for situations when you are unable to access your email.

Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Mimecast Application definition.

In this login example we are using the email as a username

After we enter the username we are prompted with another authentication method (in this example we use turing)



The image shows a login form for Mimecast. At the top is the Mimecast logo. Below it are four input fields: a username field containing 'user@mimecast.swivelsecure.com', a password field labeled 'Password', an OTC field, and a dropdown menu labeled 'TURING' with a downward arrow. Below these fields is a CAPTCHA image showing a grid of numbers. At the bottom are two buttons: 'Login' and 'Refresh Image'.

mimecast

user@mimecast.swivelsecure.com

Password

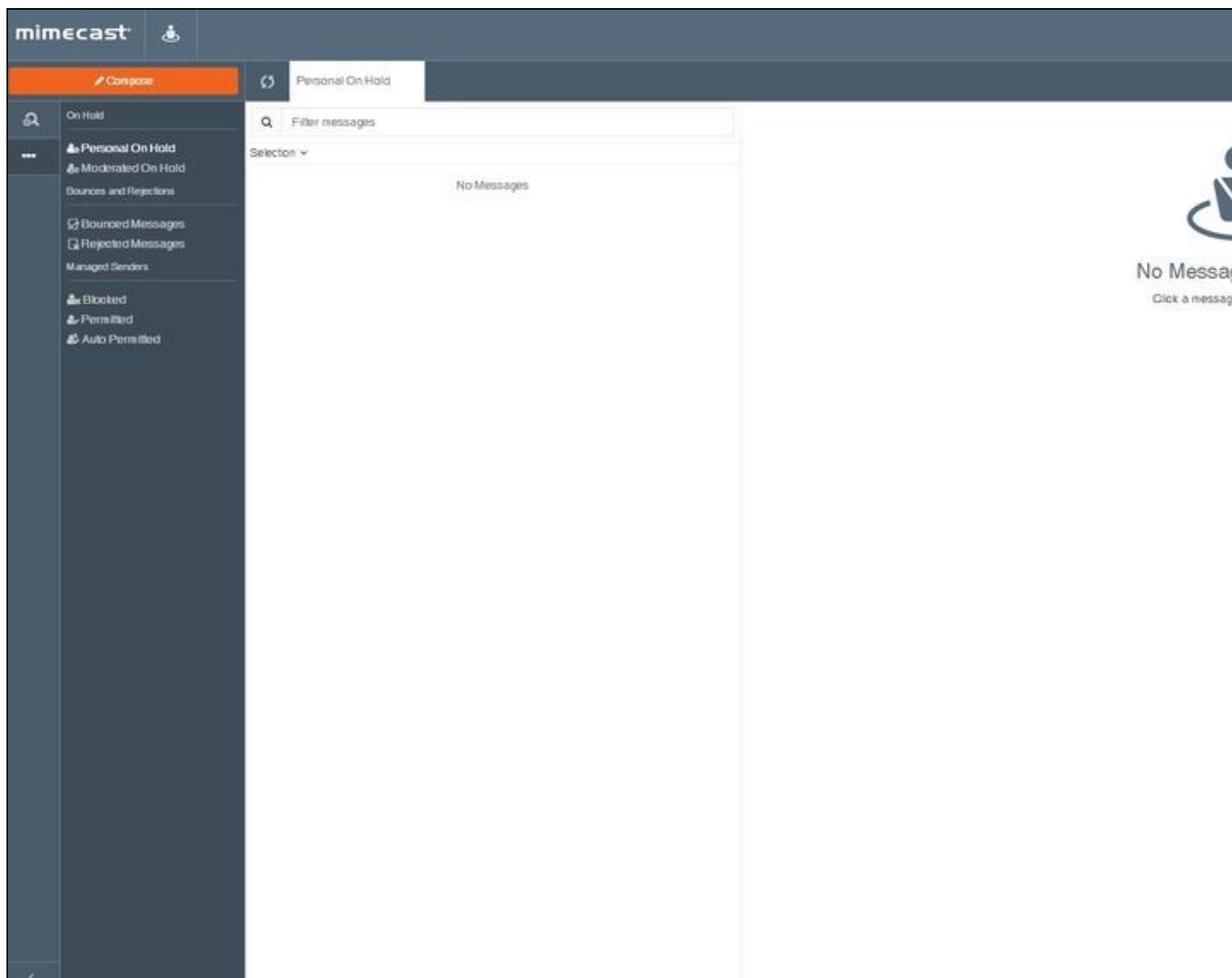
OTC

TURING

1	2	3	4	5	6	7	8	9	0
7	0	8	9	4	6	5	1	3	2

Login Refresh Image

After we enter our authentication credentials we successfully will see the Mimecast account that we tried to access.



Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Mimecast

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Metadata been uploaded to the Mimecast?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?