FortiMail Cloud Integration with Microsoft 365: Webmail SSO Deployment Guide

Version 7.4

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

https://cookbook.fortinet.com

FORTINET TRAINING SERVICES

https://www.fortinet.com/training

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February 06, 2024

TABLE OF CONTENTS

Change Log

.Date	Change Description
2024-02-06	Initial release

Introduction

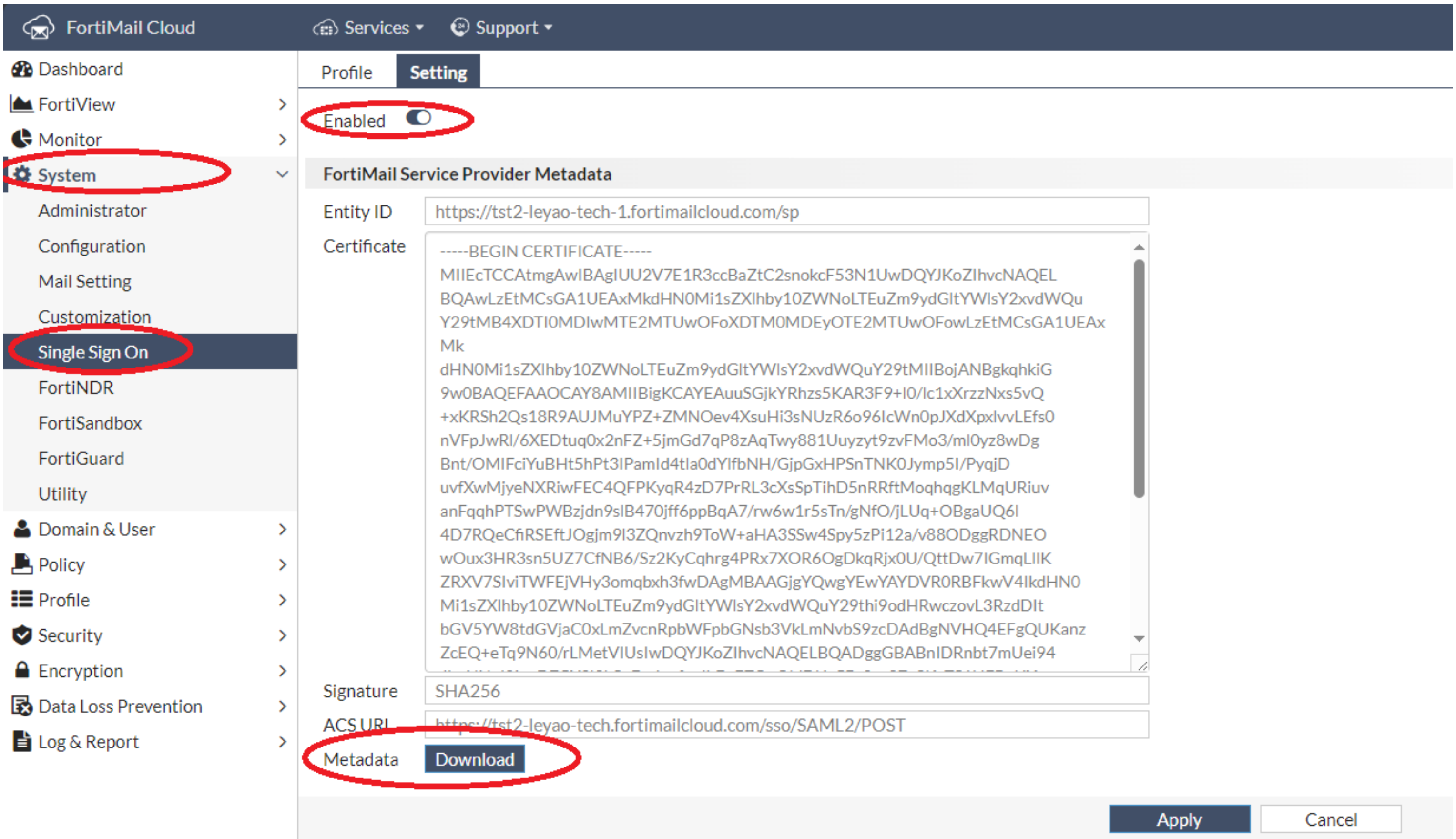
This document outlines the basic configuration steps required to integrate FortiMail Cloud with Microsoft Entra (Microsoft 365) so that users can log in to FortiMail webmail with MS365 SSO.

Note: SSO on FortiMail Cloud can only work with webmail login at the moment and does not support cloud admin login.

Creating SSO application in Microsoft Entra admin center

You must create a Docusign application on Microsoft Entra to allow the SMAL service.

1. Log in to your FortiMail Cloud Instance at FortiMail Cloud user portal: www.fortimailcloud.com
2. Go to *System* > *Single Sign On* > *Setting*.
3. Enable SMAL service and download the matadata.



Enabled ●

FortiMail Service Provider Metadata

Entity ID: https://tst2-leyao-tech-1.fortimailcloud.com/sp

Certificate:

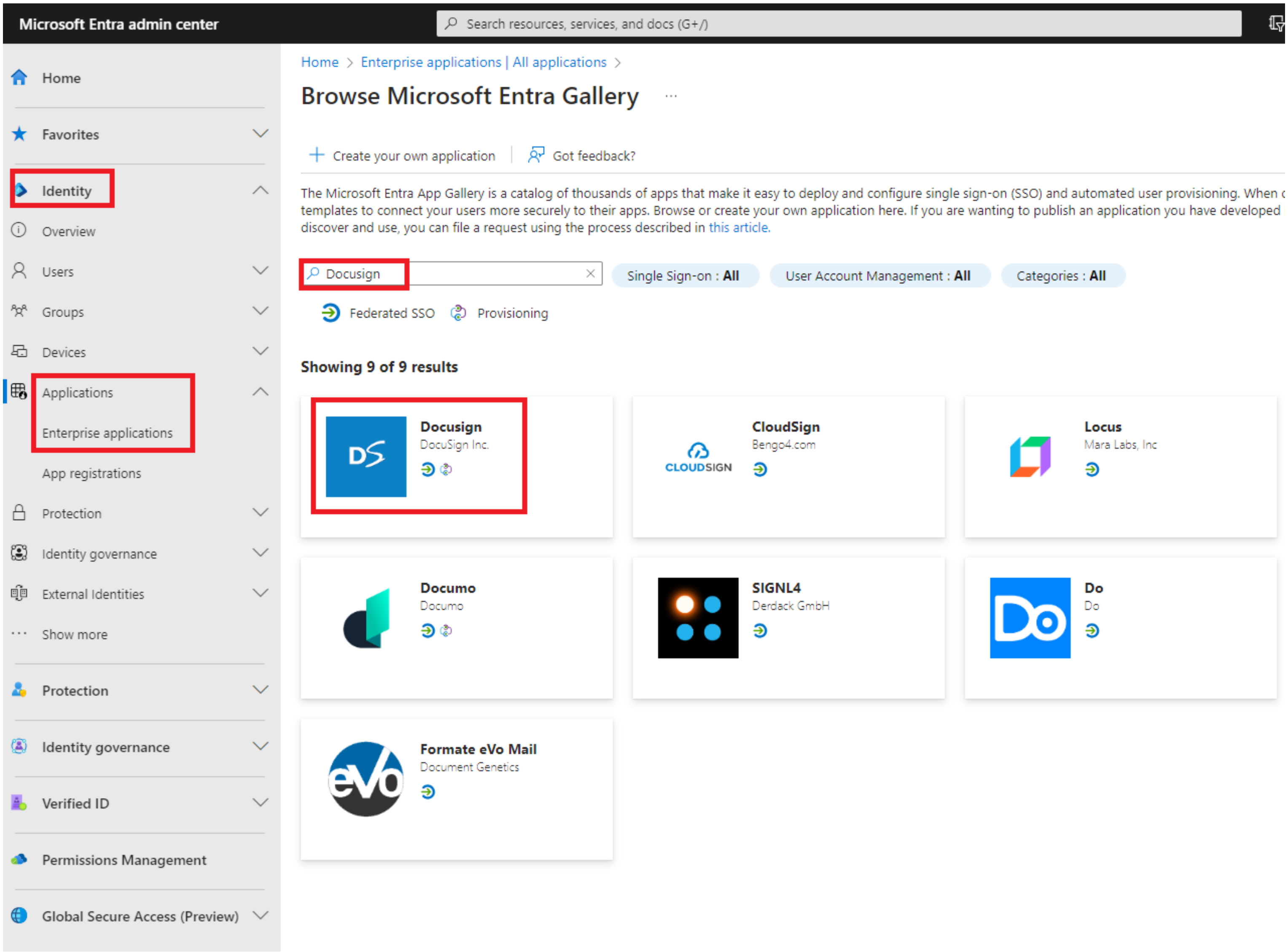
```
-----BEGIN CERTIFICATE-----
MIIEcTCCAtmgAwIBAgIUU2V7E1R3ccBaZtC2snokcF53N1UwDQYJKoZIhvcNAQEL
BQAwLzEtMCsGA1UEAxMkdHN0Mi1sZXlhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQu
Y29tMB4XDTI0MDIwMTE2MTUwOFoXDTM0MDEyOTE2MTUwOFowLzEtMCsGA1UEAx
Mk
dHN0Mi1sZXlhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQuY29tMIIBojANBgkqhkiG
9w0BAQEFAAOCAY8AMIIBigKCAYEAuuSGjkYRhzs5KAR3F9+l0/Ic1xXrzzNxs5vQ
+xKRSh2Qs18R9AUJMuYPZ+ZMNOev4XsuHi3sNUzR6o96IcWn0pJXdXpxlvvLEfs0
nVFpJwRl/6XEDtuq0x2nFZ+5jmGd7qP8zAqTwy881Uuyzyt9zvFMo3/ml0yz8wDg
Bnt/OMIFciYuBHt5hPt3IPamId4tla0dYlfbNH/GjpGxHPSnTNK0Jymp5I/PyqjD
uvfXwMjyeNXRiwFEC4QFPKyqR4zD7PrRL3cXsSpTihD5nRRftMoqhqgKLMqURiuv
anFqqhPTSwPWBzjdn9slB470jff6ppBqA7/rw6w1r5sTn/gNfO/jLUq+OBgaUQ6l
4D7RQeCfiRSEftJOgjm9I3ZQnvzh9ToW+aHA3SSw4Spy5zPi12a/v88ODggRDNEO
wOux3HR3sn5UZ7CfNB6/Sz2KyCqhrg4PRx7XOR6OgDkqRjx0U/QttDw7IGmqLIIK
ZRXV7SlviTWFEjVHy3omqbxh3fwDAgMBAAGjgYQwgYEwYAYDVR0RBFkwV4IkdHN0
Mi1sZXlhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQuY29thi9odHRwczovL3RzdDIt
bGV5YW8tdGVjaC0xLmZvcnRpbWFpbGNsb3VkLmNvbS9zcDAdBgNVHQ4EFgQUKanz
ZcEQ+eTq9N60/rLMetVIUsIwDQYJKoZIhvcNAQELBQADggGBABnIDRnbt7mUei94
```

Signature: SHA256

ACS URL: https://tst2-leyao-tech.fortimailcloud.com/sso/SAML2/POST

Metadata: Download

4. Go to Microsoft Entra admin center portal: https://entra.microsoft.com/#home
5. Go to *Identity* > *Applications* > *Enterprise applications*.
6. Click *New application*, and search for “Docusign”.



Browse Microsoft Entra Gallery

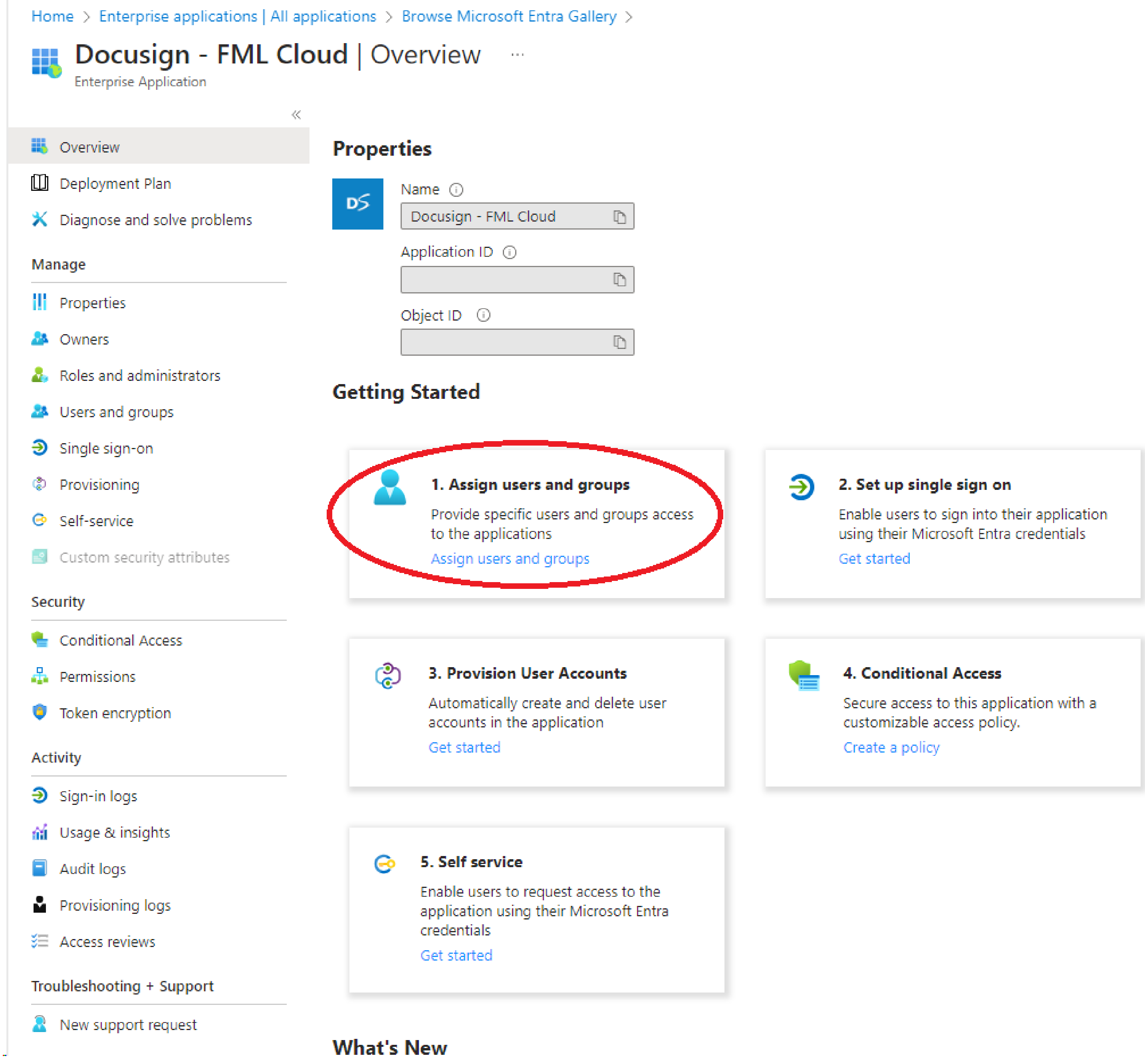
The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When c
templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed
discover and use, you can file a request using the process described in this article.

Docusign

Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Showing 9 of 9 results

7. Enter the application name (for example, “Docusign – FML Cloud”).
8. Click *Create*
9. Select *Overview* > *Assign users and groups*, then click *Add user/group* and add all users that you want grant SSO webmail access.



Name: Docusign - FML Cloud

Application ID:

Object ID:

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

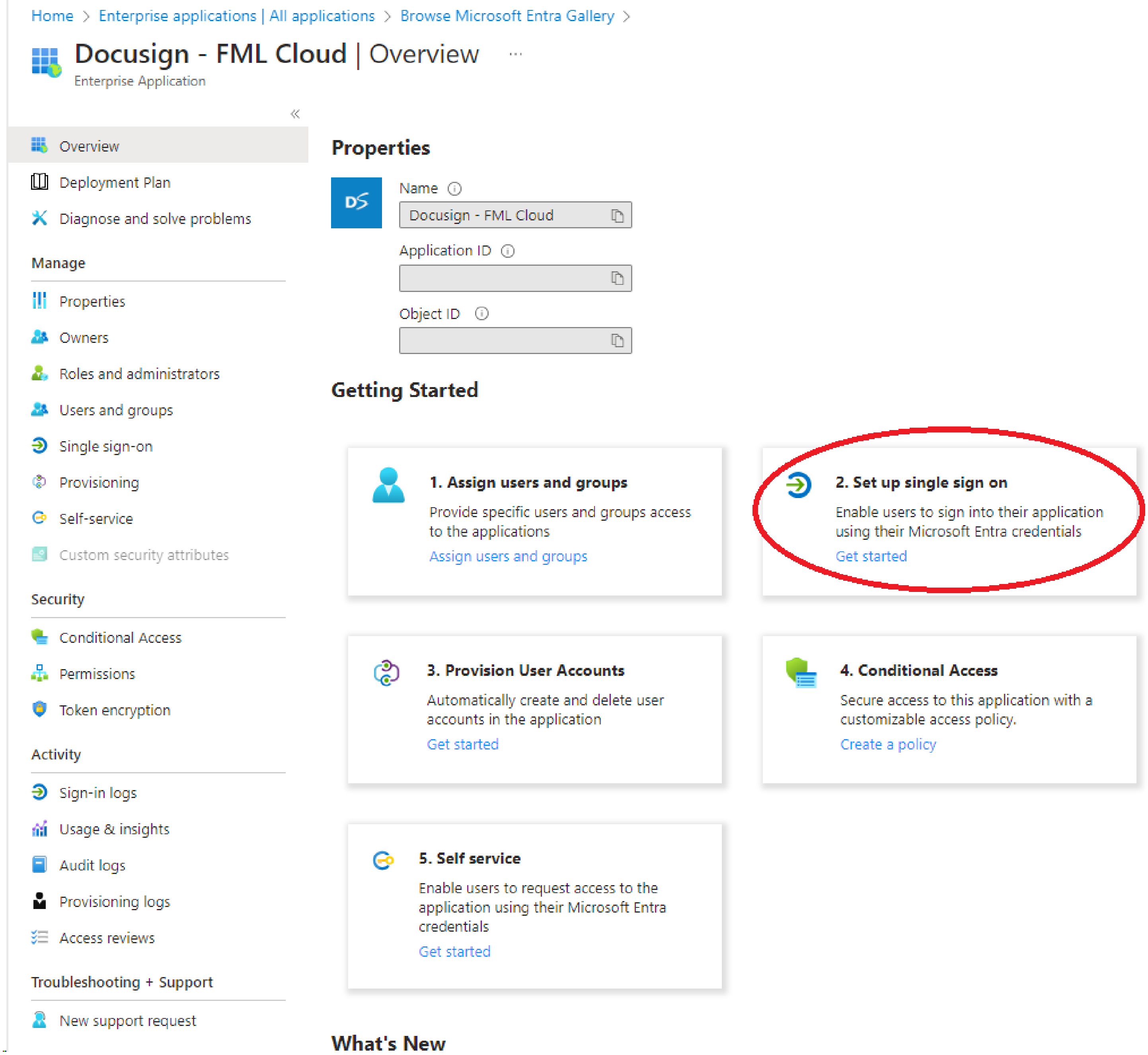
2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

10. Select *Overview* > *Set up single sign on*.



Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

Docusign - FML Cloud | Overview ...

Enterprise Application

Properties

Name: Docusign - FML Cloud

Application ID:

Object ID:

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started

3. Provision User Accounts

Automatically create and delete user accounts in the application

Get started

4. Conditional Access

Secure access to this application with a customizable access policy.

Create a policy

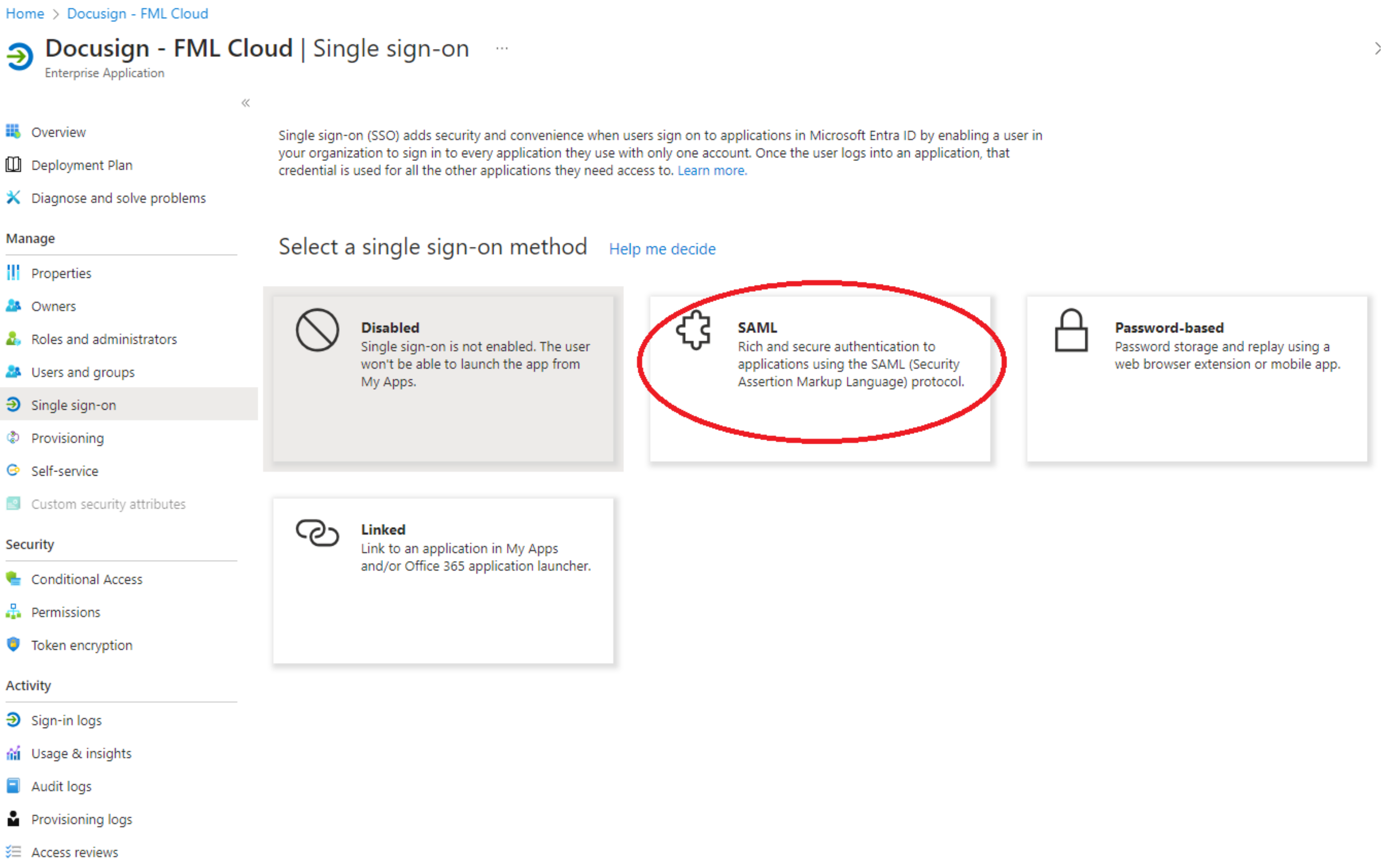
5. Self service

Enable users to request access to the application using their Microsoft Entra credentials

Get started

What's New

11. Select *SAML.*



Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

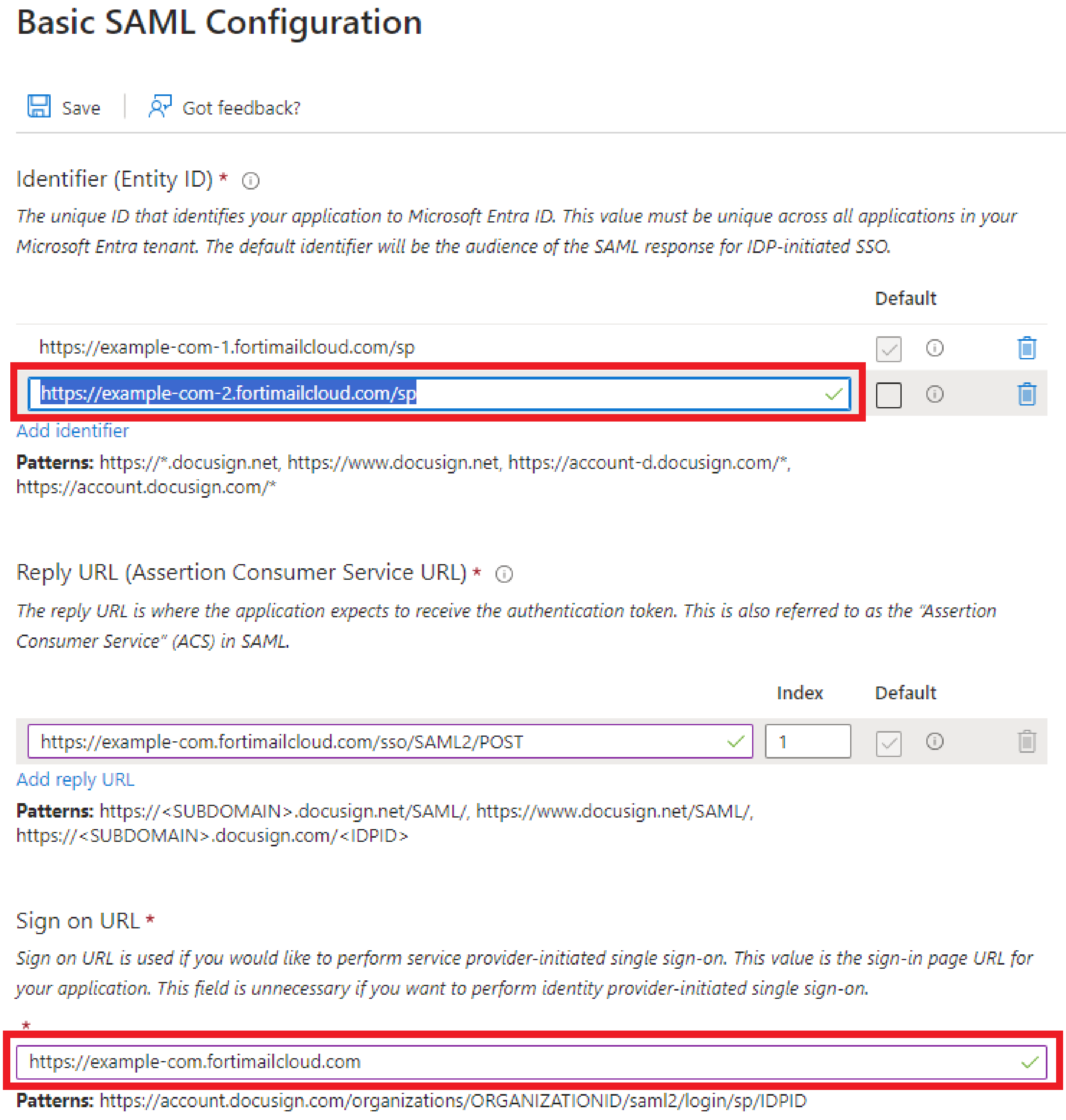
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

12. Click "*Upload metadata file*" then select the metadata file downloaded in step 3.
13. After you have uploaded the metadata, you will be prompted to *Basic SAML Configuration* automatically.

14. Click “*Add identifier*” and add a second entity ID by replacing -1 to -2 of your default entity ID.
For example, if you default ID is:
https://example-com-1.fortimailcloud.com/sp
Then add the second identifier ID as:
https://example-com-2.fortimailcloud.com/sp
Then setup *Sign on URL* as your instance hostname, example:
https://example-com.fortimailcloud.com



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://example-com-1.fortimailcloud.com/sp	☑
https://example-com-2.fortimailcloud.com/sp	□

Patterns: https://*.docusign.net, https://www.docusign.net, https://account-d.docusign.com/*, https://account.docusign.com/*

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://example-com.fortimailcloud.com/sso/SAML2/POST	1	☑

Patterns: https://<SUBDOMAIN>.docusign.net/SAML/, https://www.docusign.net/SAML/, https://<SUBDOMAIN>.docusign.com/<IDPID>

Sign on URL *

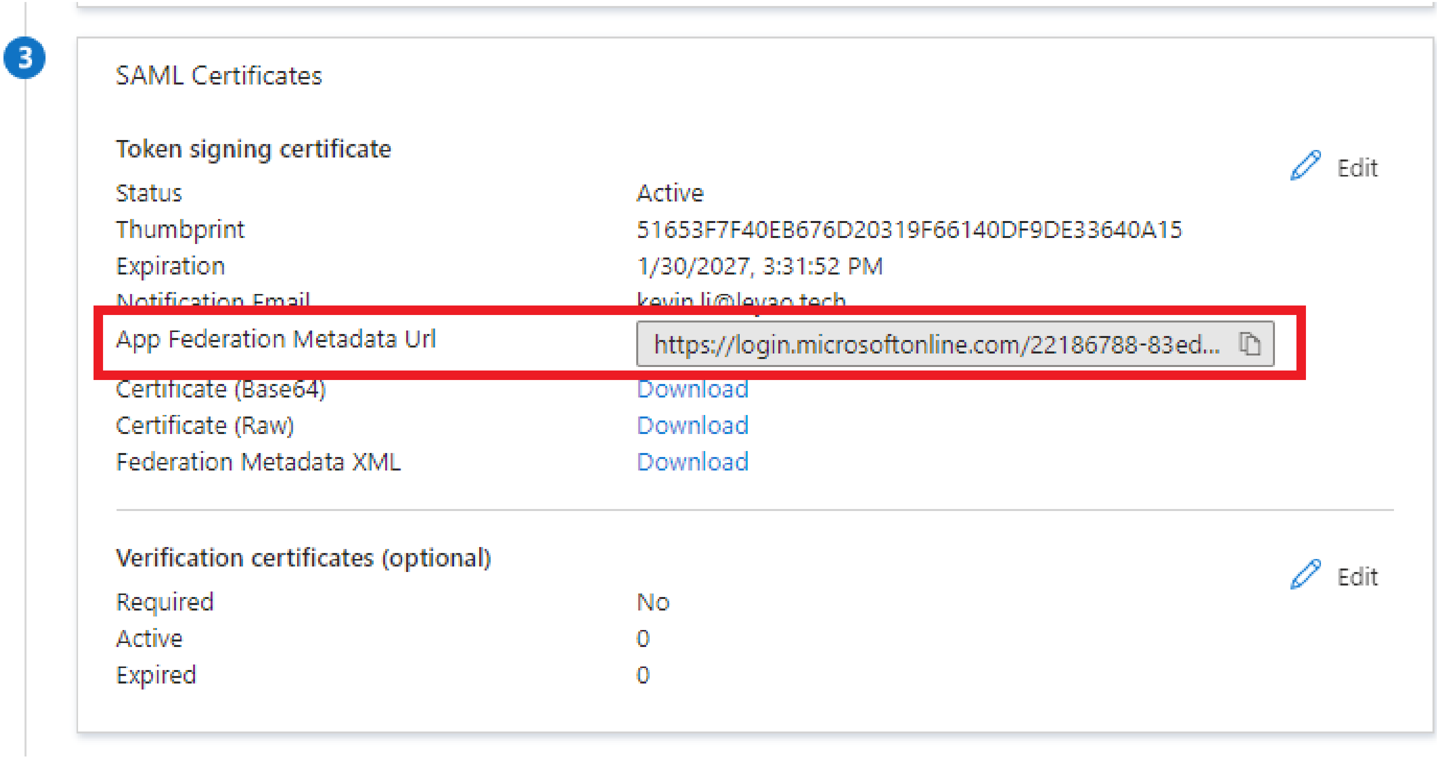
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

https://example-com.fortimailcloud.com

Patterns: https://account.docusign.com/organizations/ORGANIZATIONID/saml2/login/sp/IDPID

15. After saving the Basic SAML Configuration, copy “*App Federation Metadata URL”* from *SAML Certificates*.



SAML Certificates

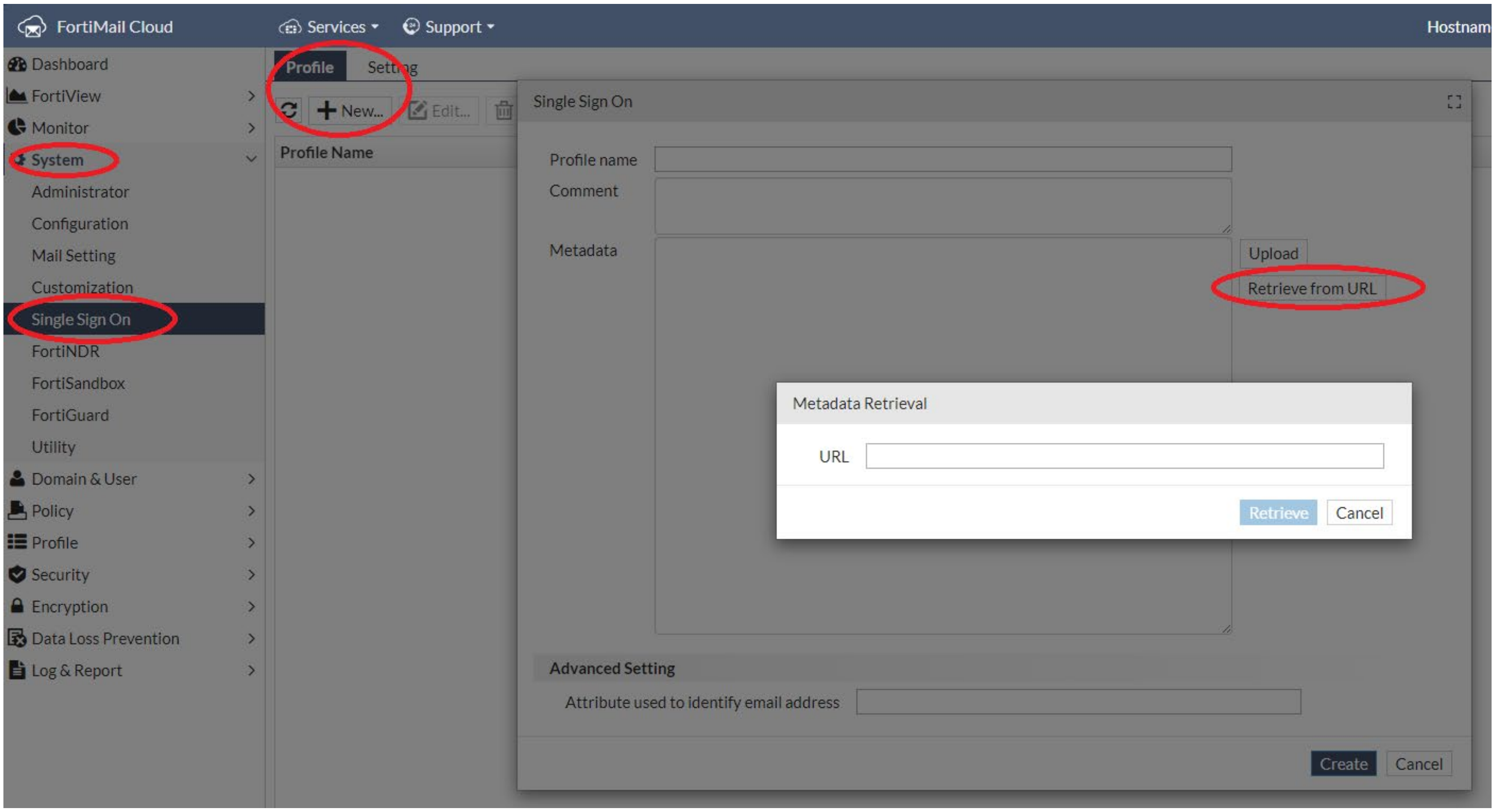
Token signing certificate

Status	Active
Thumbprint	51653F7F40EB676D20319F66140DF9DE33640A15
Expiration	1/30/2027, 3:31:52 PM
Notification Email	kevin.li@levao.tech
App Federation Metadata Url	https://login.microsoftonline.com/22186788-83ed...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

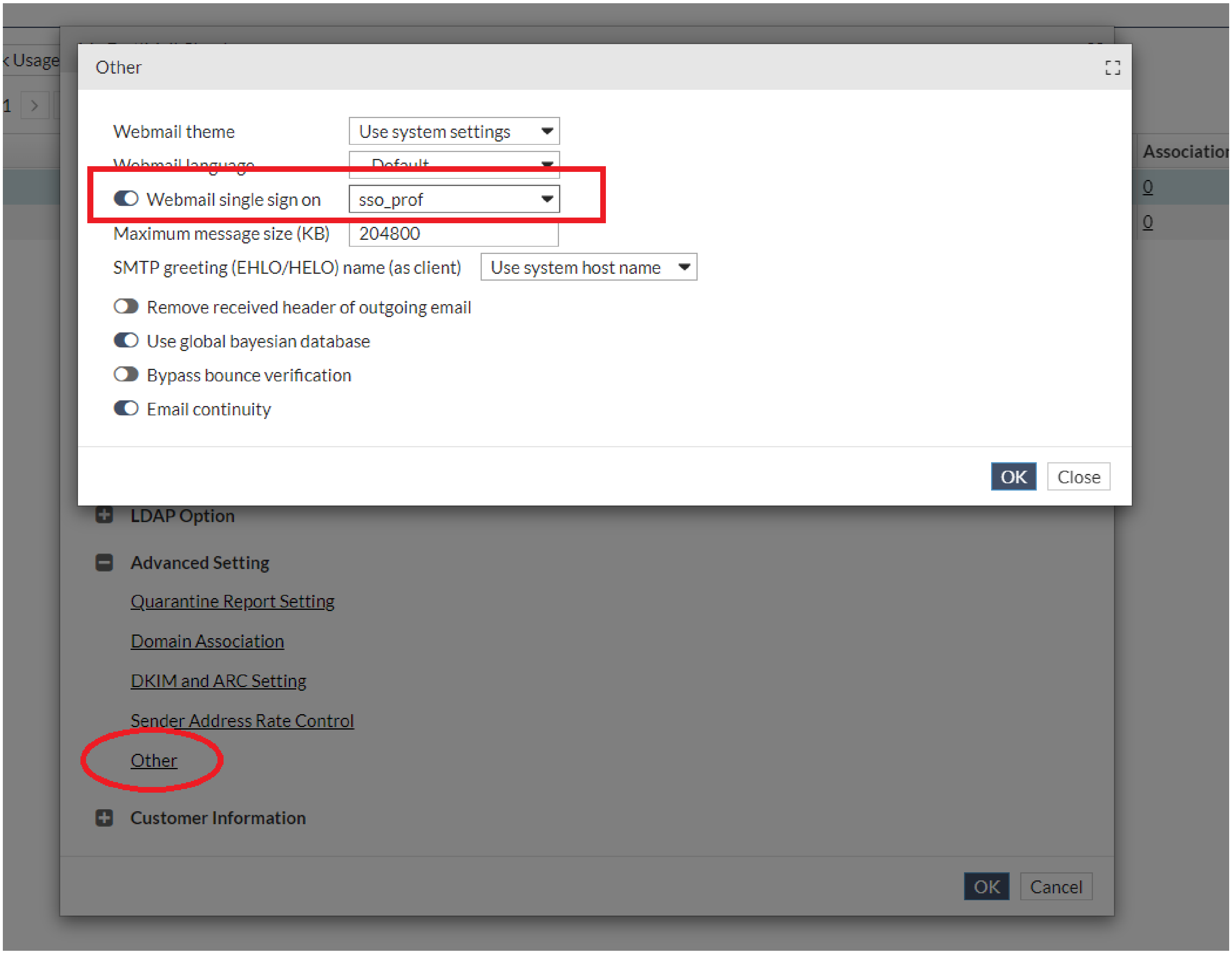
16. Log in to your FortiMail Cloud Instance at the FortiMail Cloud user portal: www.fortimailcloud.com
17. Go to *System* > *Single Sign On* > *Profile*.
18. Click *New* > *Retrieve from URL*
19. Paste the URL copies in step 15, then click *Retrieve*.



20. Then click *Create* to save the configuration.

Applying and testing SSO in FortiMail Cloud

1. Log in to your FortiMail Cloud Instance at FortiMail Cloud user portal: www.fortimailcloud.com
2. Select *Domain > select protect domain (example.com) > Advanced Setting*.
3. Click *Other* and enable *Webmail single sign on.*
4. Select the SSO profile created in the previous steps.



Other

Webmail theme: Use system settings

Webmail language: Default

● Webmail single sign on: sso_prof

Maximum message size (KB): 204800

SMTP greeting (EHLO/HELO) name (as client): Use system host name

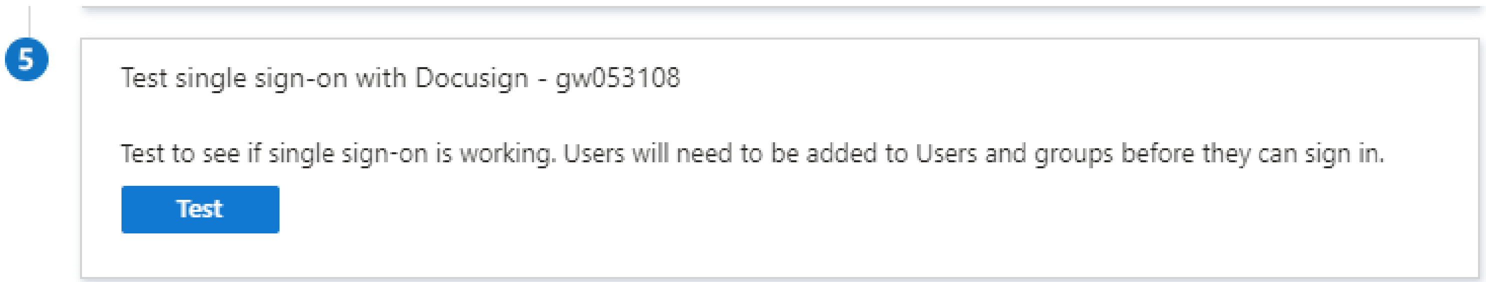
○ Remove received header of outgoing email

● Use global bayesian database

○ Bypass bounce verification

● Email continuity

5. Click *OK*.
6. Test SSO at entra.microsoft.com



5 Test single sign-on with Docusign - gw053108

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

High Performance Network Security