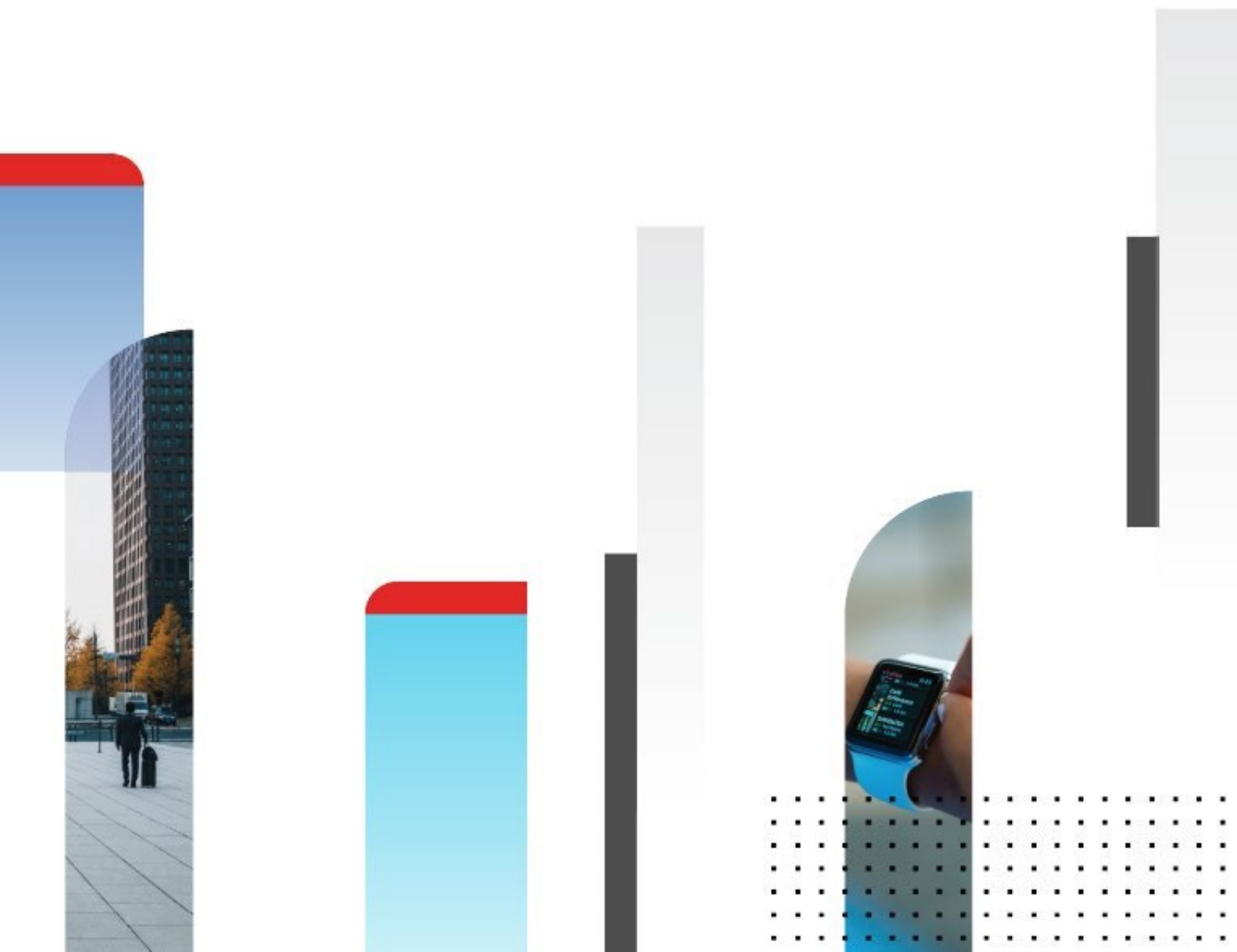


FortiMail Cloud Integration with Microsoft 365: Webmail SSO Deployment Guide

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..... 5

Introduction 6

Creating SSO application in Microsoft Entra admin center 6

Applying and testing SSO in FortiMail Cloud.....14

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 metadata.

FortiMail Cloud Services Support

Dashboard
FortiView
Monitor
System
Administrator
Configuration
Mail Setting
Customization
Single Sign On
FortiNDR
FortiSandbox
FortiGuard
Utility

Domain & User
Policy
Profile
Security
Encryption
Data Loss Prevention
Log & Report

Profile **Setting**

Enabled

FortiMail Service Provider Metadata

Entity ID

Certificate

```
-----BEGIN CERTIFICATE-----
MIIEcTCCAtmgAwIBAgIUU2V7E1R3ccBaZtC2snokcF53N1UwDQYJKoZIhvcNAQEL
BQAwLzEtMCsGA1UEAxMkdHN0Mi1sZXIhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQu
Y29tMB4XDTI0MDIwMTE2MTUwOFoXDTE0MDEyOTE2MTUwOFowLzEtMCsGA1UEAxMk
dHN0Mi1sZXIhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQuY29tMIIBojANBgkqhkiG
9w0BAQEFAAOCAy8AMIIBigKCAYEAuuSGjkYRhzs5KAR3F9+IO/lc1xXrzzNxs5vQ
+XKRSh2Qs18R9AUJMuYPZ+ZMNOev4XsuHi3sNUzR6o96lcWn0pJdXdpXlvvLEfs0
nVFPJwRI/6XEDtuq0x2nFZ+5jmGd7qP8zAqTwy881Uuyzyt9zvFMo3/ml0yz8wDg
Bnt/OMIFciYuBHt5hPt3IPamld4tla0dYlfbNH/GjpGxHPSnTNK0Jymp5I/PyqID
uvrXwMjyeNXRiweFEC4QFPKyr4zD7PrRL3cXsSpTihD5nRRftMoghqgKLMqURiuv
anFqhqPTswPWBzjdn9slB470jff6ppBqA7/rw6w1r5sTn/gNfo/jLUq+OBgaUQ6l
4D7RQeCfrSEfJogjm9l3ZQnvzh9ToW+ahA3S5w4Spy5zPi12a/v88ODggRDNEO
wOux3HR3sn5UZ7cfnB6/Sz2KyCqhrG4PRx7XOR6OgDkqRjx0U/QttDw7IGmqLIik
ZRxV7SlviTWFEjVHy3omqbhx3fwDAgMBAAGjYQwgYEWYAYDVR0RBfkwV4lkdHNO
Mi1sZXIhby10ZWNoLTEuZm9ydGltYWlsY2xvdWQuY29thi9odHRwczovL3RzdDlt
bGV5YW8tdGVjaC0xLmZvcnRpbWFPbGNSb3VklmNvbS9zcDAdBgNVHQ4EFgQUKanz
ZcEQ+eTq9N60/rLMetVIUslwDQYJKoZIhvcNAQELBQADggGBABnIDRnbt7mUei94
-----
```

Signature

ACSURL

Metadata **Download**

Apply **Cancel**

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”.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane shows the 'Identity' and 'Applications' sections highlighted with red boxes. The 'Applications' section is expanded, showing 'Enterprise applications' as the selected option. The main content area is titled 'Browse Microsoft Entra Gallery' and shows search results for 'DocuSign'. The search bar contains 'DocuSign', and the results list includes 'DocuSign', 'CloudSign', 'Locus', 'Documo', 'SIGNL4', 'Do', and 'Formate eVo Mail'. The 'DocuSign' application is highlighted with a red box.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?

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 you use 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 to 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

Federated SSO | Provisioning

Showing 9 of 9 results

- DocuSign**
DocuSign Inc.
- CloudSign**
Bengo4.com
- Locus**
Mara Labs, Inc.
- Documo**
Documo
- SIGNL4**
Derdack GmbH
- Do**
Do
- Formate eVo Mail**
Document Genetics

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.

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

DocuSign - FML Cloud | Overview

Enterprise Application

«

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs


Provisioning logs

Access reviews

Troubleshooting + Support

New support request


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


10. Select Overview > Set up single sign on.


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

Docusign - FML Cloud | Overview ...


Enterprise Application


Overview


 Deployment Plan


 Diagnose and solve problems


Manage


 Properties


 Owners

 Roles and administrators

 Users and groups


 Single sign-on


 Provisioning


 Self-service

 Custom security attributes


Security


 Conditional Access


 Permissions


 Token encryption


Activity

 Sign-in logs


 Usage & insights

 Audit logs

 Provisioning logs

 Access reviews

Troubleshooting + Support

 New support request

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.

Home > Docusign - FML Cloud

 **Docusign - FML Cloud** | Single sign-on ...
Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

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 [Help me decide](#)



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

 Save |  Got feedback?

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	<input checked="" type="checkbox"/> ⓘ 
https://example-com-2.fortimailcloud.com/sp	<input type="checkbox"/> ⓘ 

[Add identifier](#)

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	<input checked="" type="checkbox"/> ⓘ 

[Add reply URL](#)

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*.

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

51653F7F40EB676D20319F66140DF9DE33640A15


Expiration

1/30/2027, 3:31:52 PM

Notification Email

kevin.li@leyao.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

 Edit

 Edit

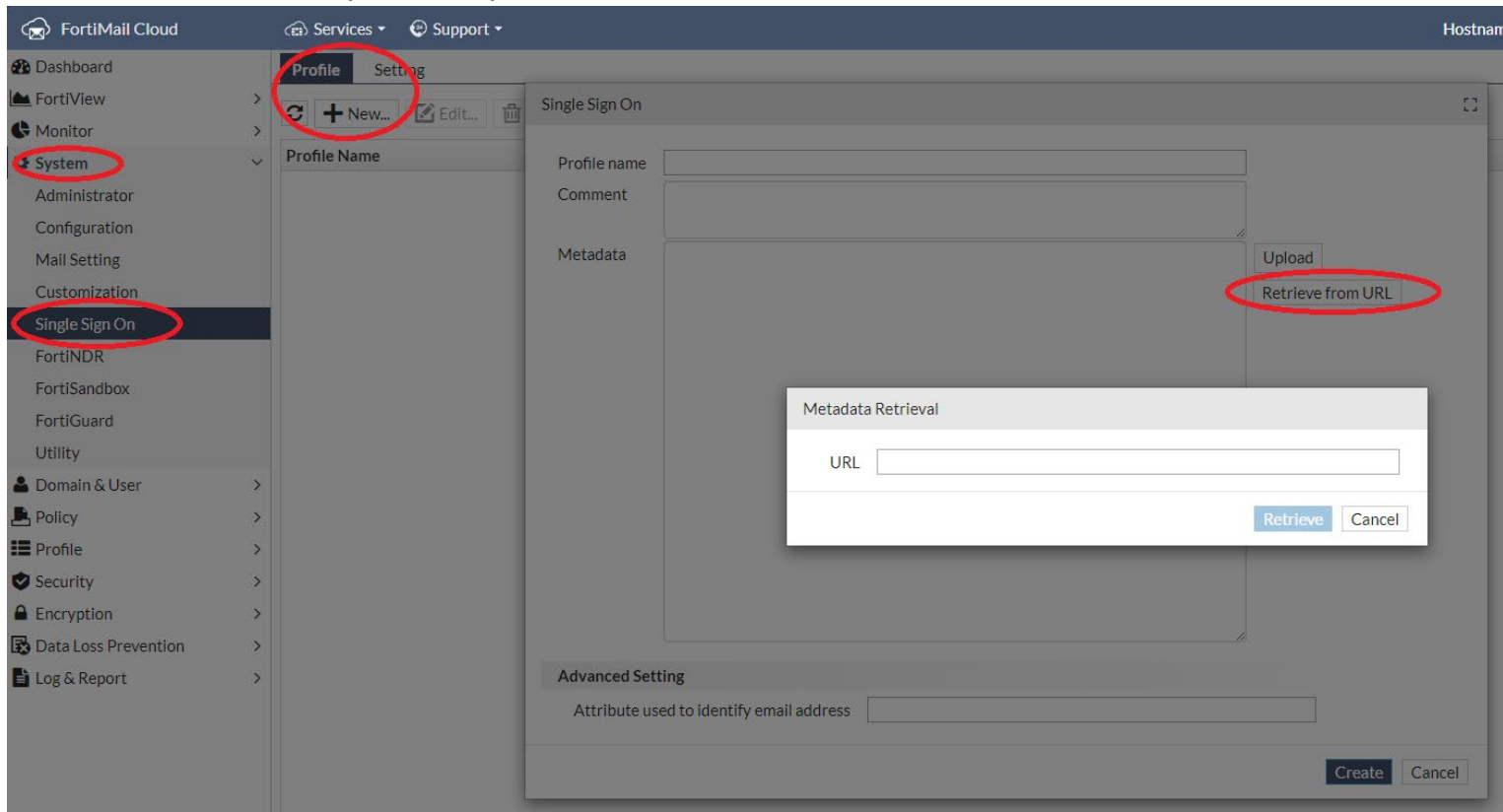
16. Log in to your FortiMail Cloud Instance at the FortiMail Cloud user portal:

www.fortimailcloud.com

17. Go to *System > Single Sign On > Profile*.

18. Click *New > Retrieve from URL*

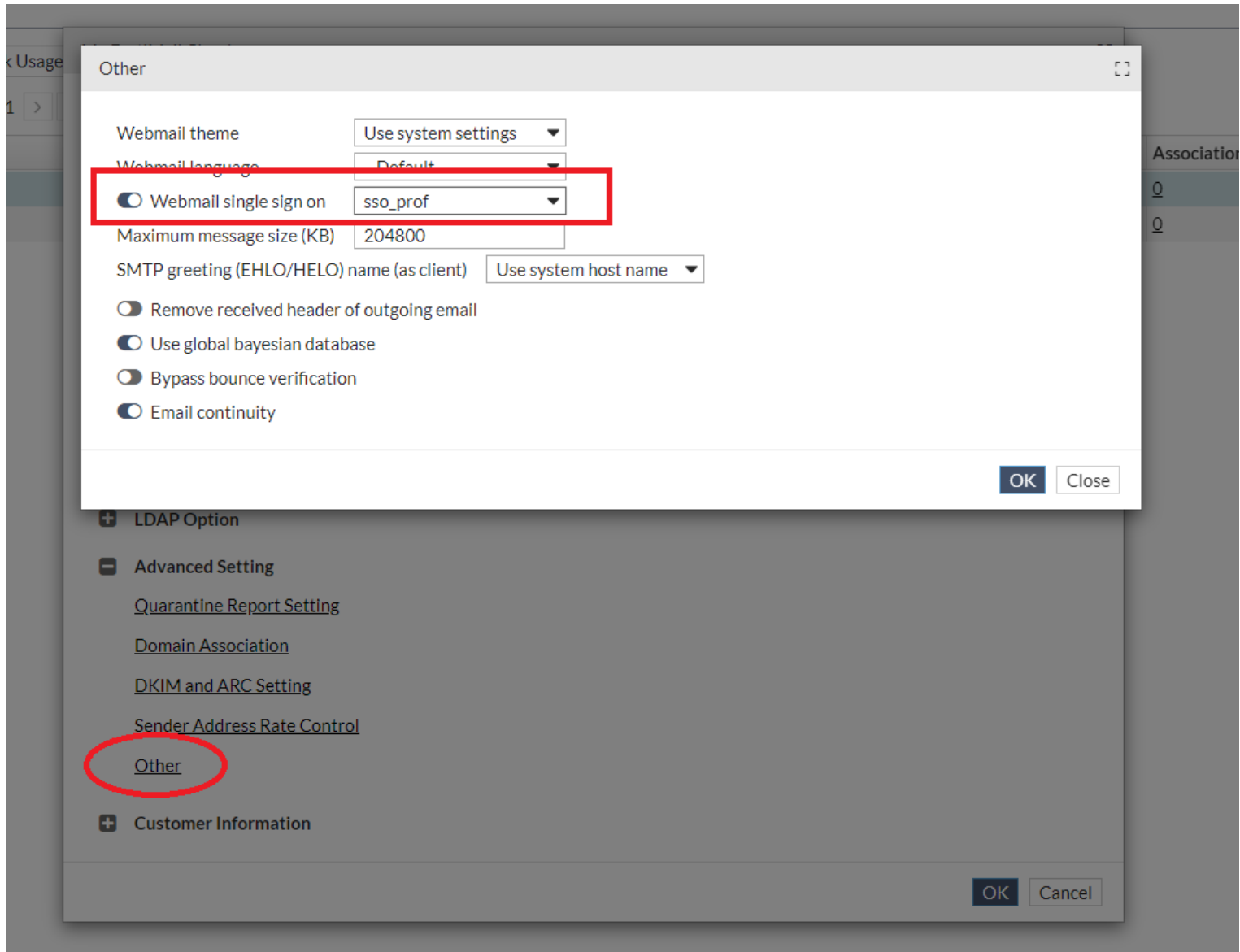
19. Paste the URL copies in step 15, then click *Retrieve*.



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.



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.

Test



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.