



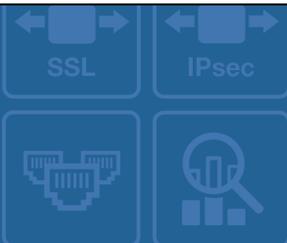
FORTINET

High Performance Network Security



FortiMail™ SSO With Centrify Setup Guide

Version 5.4



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



August 1, 2017

TABLE OF CONTENTS

1. Prerequisite Configurations.....	4
2. How to Configure Centrify	5
3. How to Enable FortiMail Webmail Single Sign On	9

This document describes how to configure FortiMail Webmail Single Sign On to work with Centrify.

1. Prerequisite Configurations

The FortiMail unit should have been configured properly for sending and receiving email messages. Please make sure the following three conditions are met:

- The FortiMail unit is running in Server Mode
- A protected domain has been configured to host mail users
- All email users have been configured either locally or using an LDAP profile (LDAP profile is recommended)

Follow the below steps to configure the LDAP profile and protected domain if necessary:

1.1. Go to **Profile > LDAP** and create a new LDAP profile.

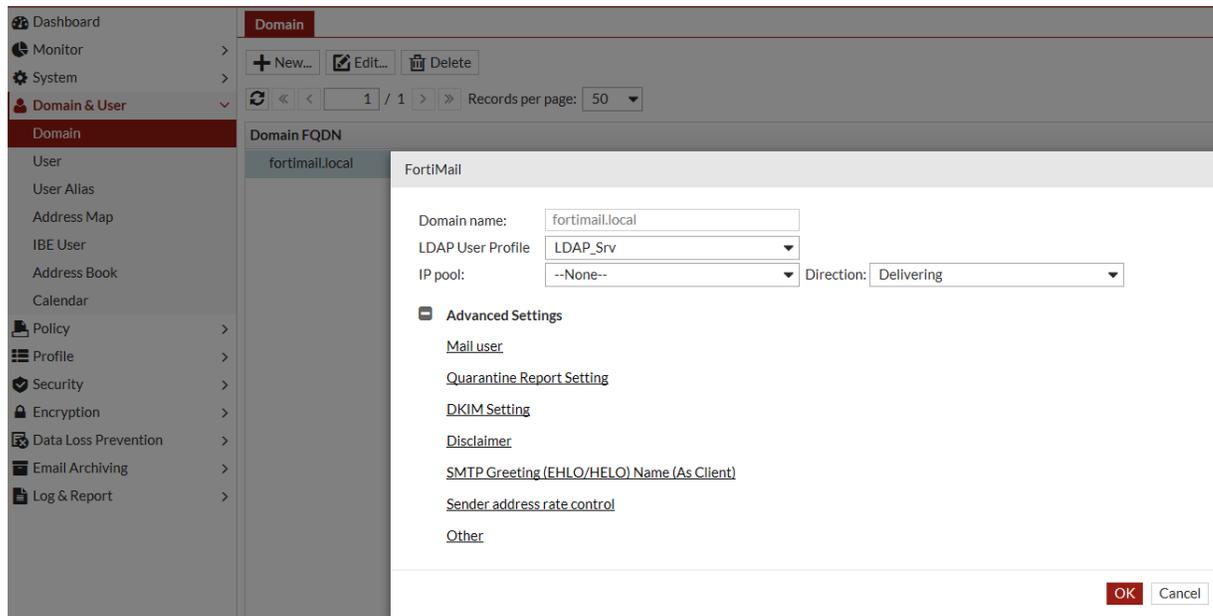
1.2. Configure **Server, Base DN, Bind DN, Bind Password**, and set **User query** so that FortiMail can verify user properly with the LDAP server. For example:

((userPrincipalName=\$m)(mail=\$m))

The screenshot shows the 'Edit LDAP Profile' configuration page in the FortiMail web interface. The profile name is 'LDAP_Srv'. The server name/IP is '172.20.140.191' and the port is '389'. The fallback server name/IP is empty and the port is '389'. The 'Use secure connection' is set to 'None'. The 'Default Bind Options' section shows 'Base DN' as 'cn=users,dc=fortimail,dc=local', 'Bind DN' as 'cn=administrator,cn=users,dc=fortimai', and 'Bind password' as masked with dots. The 'User Query Options' section shows the 'User query' as '((userPrincipalName=\$m)(mail=\$m))', 'Scope' as 'Subtree', and 'Derefer' as 'Never'. There are also sections for 'Group Query Options', 'User Authentication Options', and 'User Alias Options' which are currently disabled.

1.3. Go to **Domain & User > Domain**.

1.4. Create a domain with your domain name, and select the previously created LDAP profile in “LDAP User Profile”.



1.5 Enable SAML on FortiMail CLI with the following CLI commands:

```
config system saml
    set status enable
end
```

2. How to Configure Centrify

Note: Screen captures in this section are for reference only.

2.1. Add Centrify Connector

Log in to Centrify cloud account. In the console tree, go to **Settings > Network**, and click **Add Centrify Connector** to download the installation package to install on an Active Directory server.

- Customization
- Mobile
- Authentication
- Network**
 - Centrify Connectors
 - Corporate IP Range
 - SafeNet KeySecure Configuration

Centrify Connectors [Learn more](#)

Use these settings to add and manage connectors.

Add Centrify Connector

	Name	Forest	Version	Last Ping
<input type="checkbox"/>	WIN-C7CVTRPEND0	fortimail.local	17.4.148	05/15/2017 09:13 AM

Add Centrify Connector ✕



1 DOWNLOAD

Download the appropriate connector package for your system.





2 INSTALL

Install the connector package on the target server.

[View Help](#)

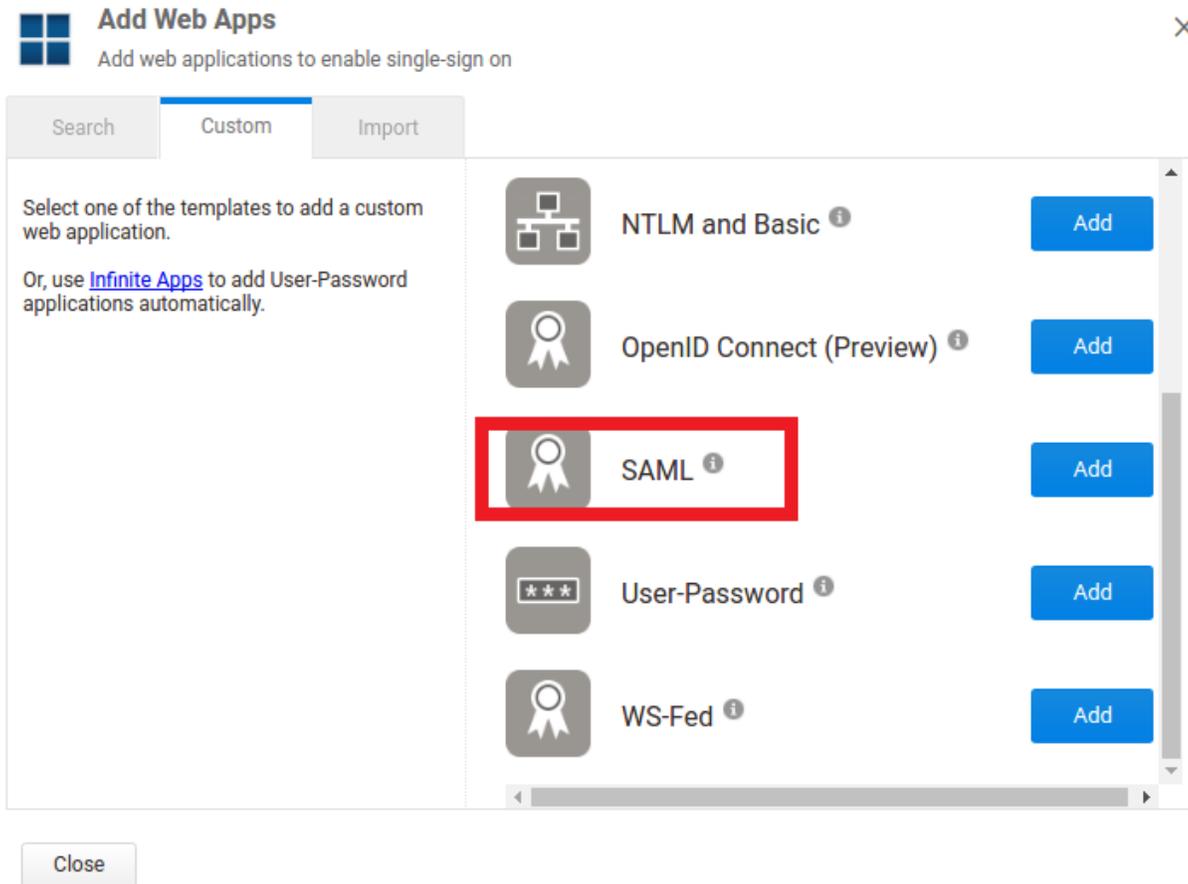


3 REGISTER

Enter your admin user name and password when prompted.

Close

2.2 On the **Apps** page, add custom app **SAML** and apply to everyone.



2.3 Double click the **SAML** app added in the above step 2.2, and click **Upload SP Metadata** to upload the FortiMail Metadata. After enabling SAML in FortiMail, you can download FortiMail Metadata from such a link:

https://fortimail_ip_or_host/sso/Metadata

2.4 Copy Identity Provider SAML Meta data URL of Centrify to be used later (in step #3.5)

The screenshot displays the 'Application Settings' page for a SAML application. The interface includes a top navigation bar with 'Dashboards', 'Users', 'Apps', 'Devices', 'Policies', 'Roles', 'Reports', 'Requests', and 'Settings'. The 'Apps' section is active, showing 'SAML' (Web - SAML, Deployed) with an 'Actions' dropdown and 'Application Configuration Help'. A left sidebar lists navigation options: 'Application Settings', 'Description', 'User Access', 'Policy', 'Account Mapping', 'Advanced', 'App Gateway', 'Changelog', and 'Workflow'. The main content area is titled 'Application Settings' and contains several sections:

- Service Provider Info:** Includes an 'Upload SP Metadata' button and an 'Assertion Consumer Service URL' field with the value 'https://[redacted]so/SAML2/POST'.
- Issuer:** A field containing 'https://aar0410.my.centrixy.com/cceb1498-261d-4f8d-a412-a595500bb0aE'.
- Encrypt Assertion:** A checkbox that is currently unchecked, with an 'Encryption Certificate' section below it containing a 'Filename' field, 'Browse', and 'Clear' buttons.
- Identity Provider Info:** Contains several URL fields:
 - Identity Provider Sign-in URL:** 'https://aar0410.my.centrixy.com/applogin/appKey/cceb1498-261d-4f8d-a4'
 - Identity Provider Error URL:** 'https://aar0410.my.centrixy.com/uperror?title=Error%20Signing%20in&mes:'
 - Identity Provider Sign-out URL:** 'https://aar0410.my.centrixy.com/applogout'
 - Download Identity Provider SAML Meta data:** A link to download the metadata.
 - Identity Provider SAML Meta data URL:** This field is highlighted with a red box and contains the URL 'https://aar0410.my.centrixy.com/saasManage/DownloadSAMLMetadataFo'.
- Download Signing Certificate:** A link to download a certificate with the thumbprint 'CN=Centrixy Customer AAR0410 Application Signing Certificate Thumbprint 26E2B5D78628109E1523BAAD4C2DAD52F10125D4'.

At the bottom of the settings area are 'Save' and 'Cancel' buttons.

2.5 Add customized mapping rule on Centrify.

Add below rule to your SAML Advanced setting:

```
setAttribute("urn:oid:0.9.2342.19200300.100.1.3", LoginUser.Get("mail"));
```

Dashboards Users **Apps** Devices Policies Roles Reports Requests Settings

Apps

SAML
Web - SAML Deployed
Actions

Application Settings
Description
User Access
Policy
Account Mapping
Advanced
App Gateway
Changelog
Workflow

Advanced [Learn more](#)

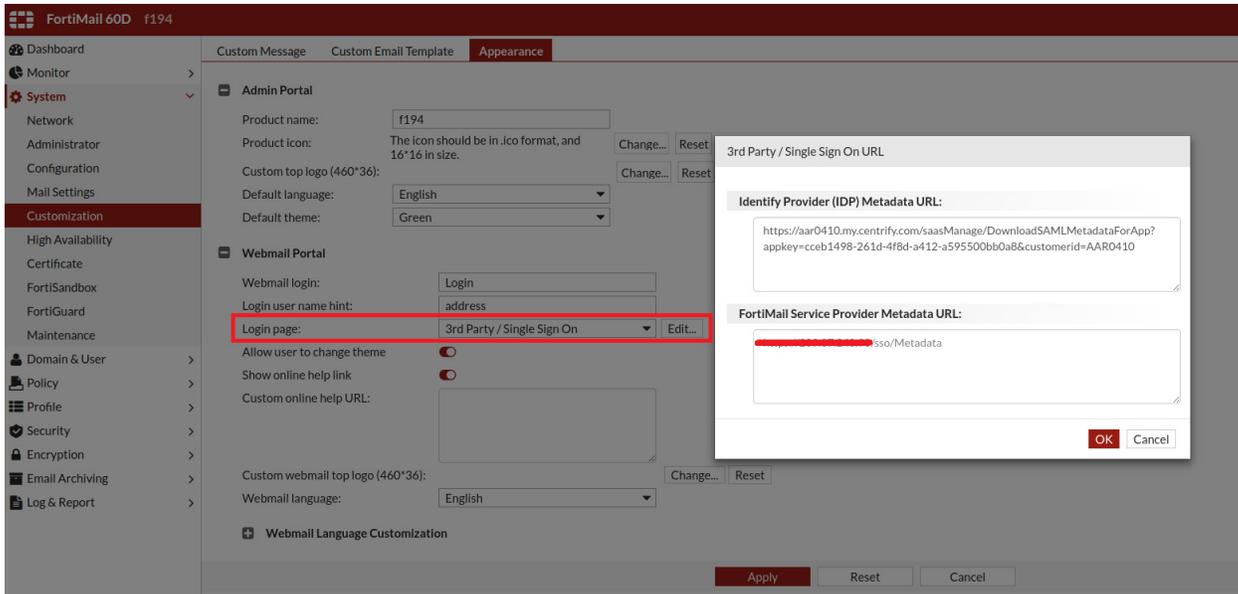
Reset Script Test

Script to generate a SAML assertion for this application

```
1 setIssuer(Issuer);  
2 setSubjectName(UserIdentifier);  
3 setAudience('https://FE-6003915000125/sp');  
4 setRecipient(ServiceUrl);  
5 setHttpDestination(ServiceUrl);  
6 setSignatureType('Response');  
7 setAttribute("urn:oid:0.9.2342.19200300.100.1.3", LoginUser.Get("mail"));
```

3. How to Enable FortiMail Webmail Single Sign On

- 3.1. Go to **System** --> **Customization** --> **Appearance** in the Advanced Mode of FortiMail admin GUI.
- 3.2. Expand **Web Portal** section and locate **Login page**: drop down list
- 3.3. Select **3rd Party / Single Sign On** option, and click on 'Edit...' button to set the IDP Metadata URL.
- 3.4. Copy the Identity Provider URL from Centrify (from step #2.4) in the text area "Identify Provider (IDP) Metadata URL:" and click **OK**.



Notes:

- Once SSO is enabled, all user login authentication will be controlled by the Active Directory, not by FortiMail. Disabled user accounts will not be authenticated by the Active Directory.
- Once SSO is enabled, user account status and mobile access status settings in the resource profile will be discarded when accessing FortiMail Webmail Portal.
- Once SSO is enabled, FortiMail Webmail portal must be accessed using HTTPS (i.e. https://fortimail_ip_or_hostname)
- Currently, logging out FortiMail Webmail will also log out user from IDP in the case of SSO.

Recommended Browsers:

Latest version of Google Chrome, FireFox and Edge browsers.

FORTINET

High Performance Network Security



Copyright© 2016 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.