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

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:

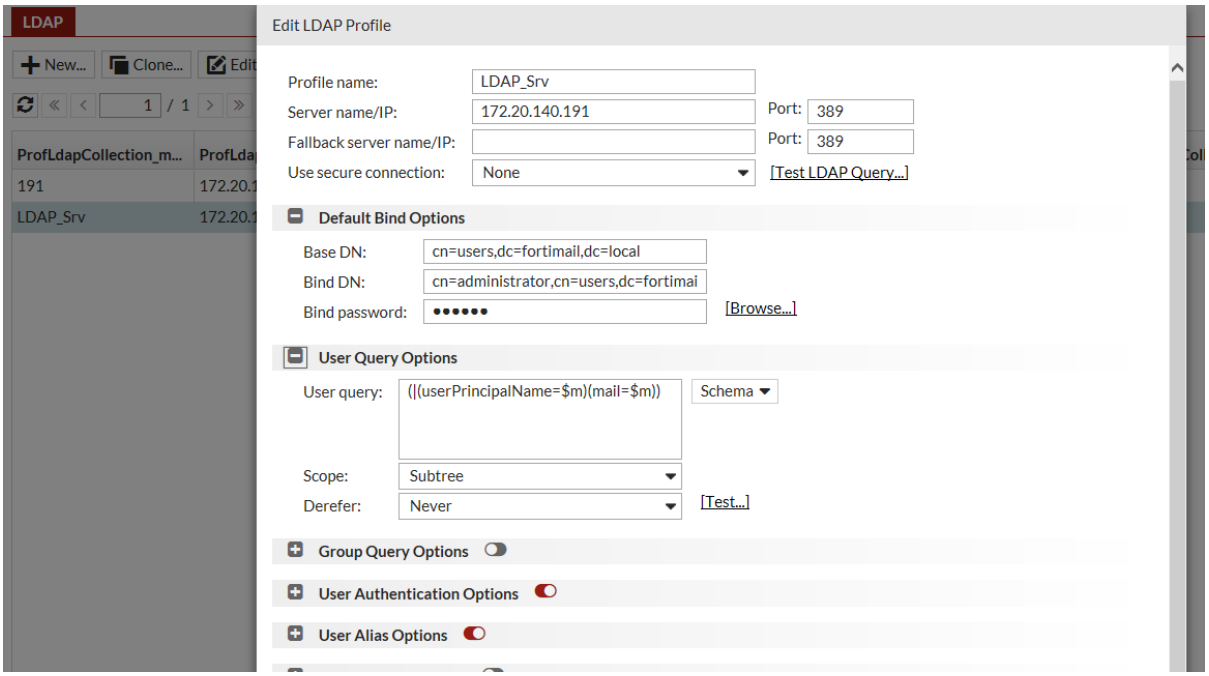
- The FortiMail unit is running in Server Mode
- A protected domain has been configured to host mail users
- All email users have been configured either locally or using an LDAP profile (LDAP profile is recommended)

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.

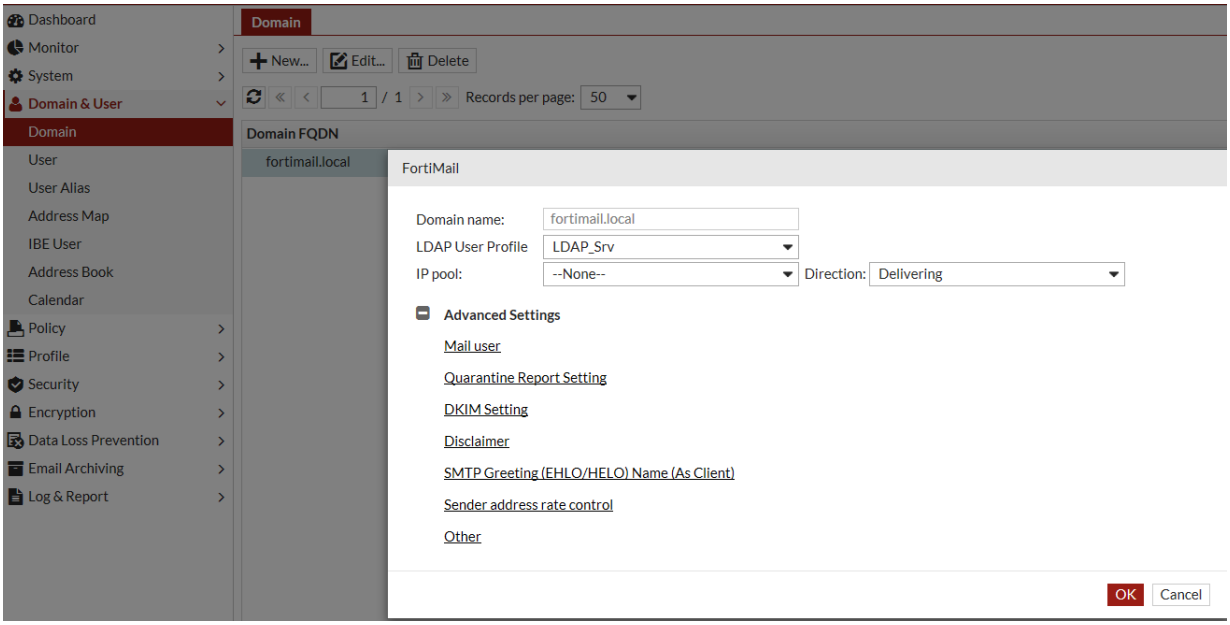
1.2. Configure **Server**, **Base DN**, **Bind DN**, **Bind Password**, and set **User query** so that FortiMail can verify user properly with the LDAP server. For example:

(|(userPrincipalName=$m)(mail=$m))



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 sytem saml

  set status enable

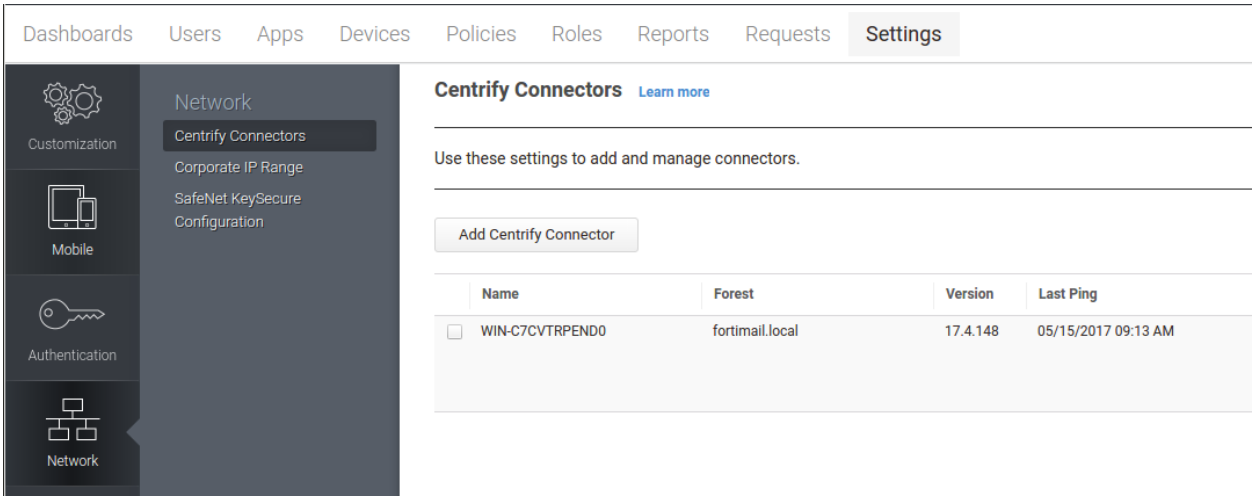
end

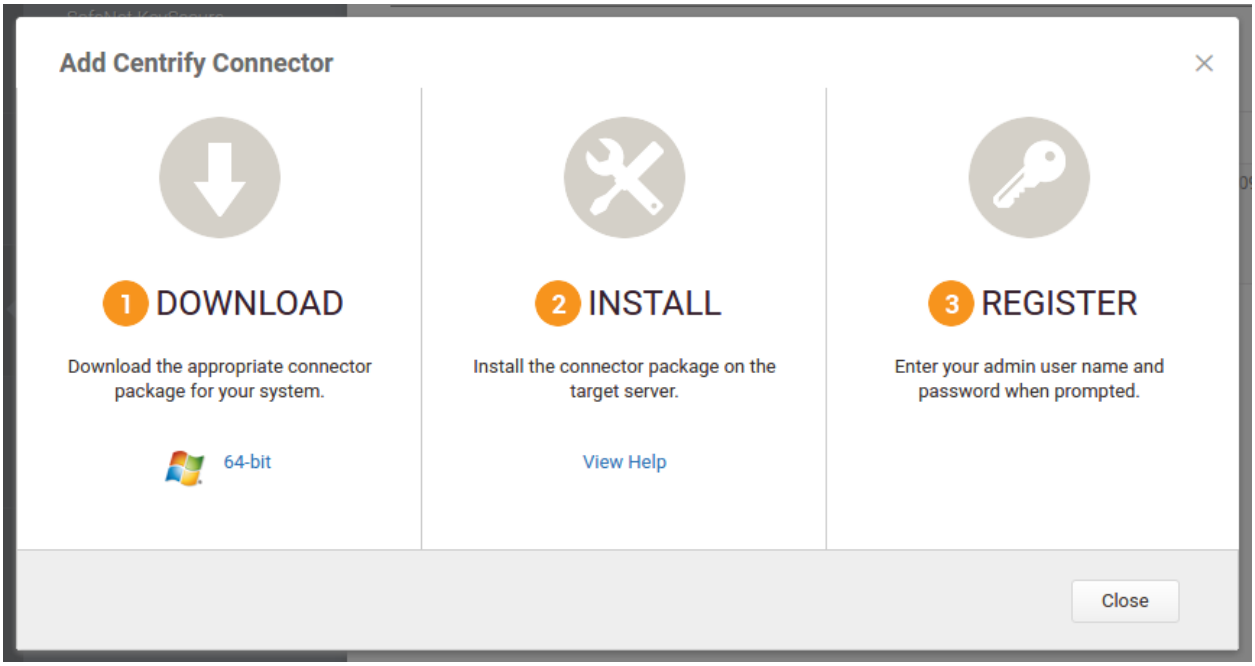
2. How to Configure Centrify

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

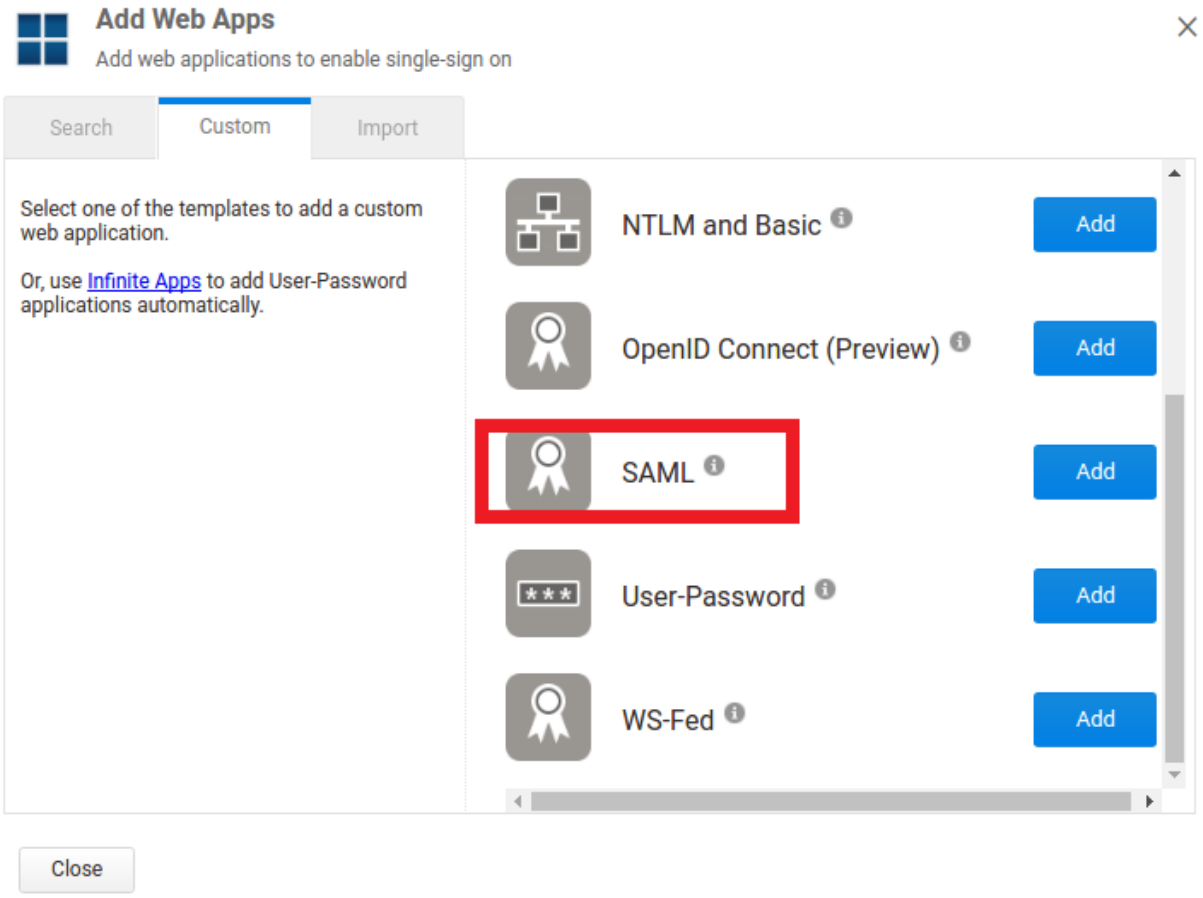
2.1. Add Centrify Connector

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.


Dashboards
Users
Apps
Devices
Policies
Roles
Reports
Requests
Settings
Customization
Mobile
Authentication
Network
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
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.
64-bit
2 INSTALL
Install the connector package on the target server.
View Help
3 REGISTER
Enter your admin user name and password when prompted.
Close

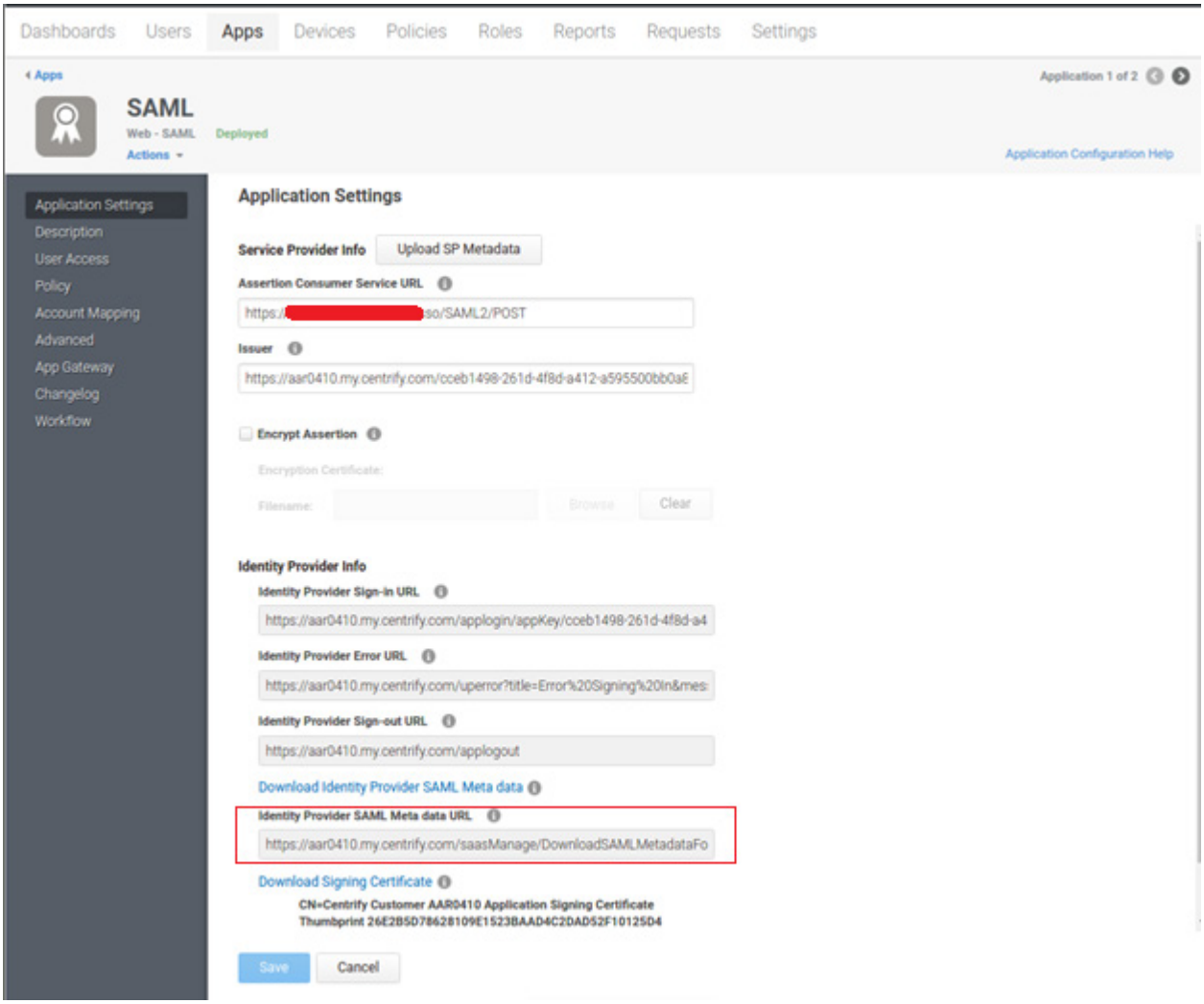
2.2 On the **Apps** page, add custom app **SAML** and apply to everyone.



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

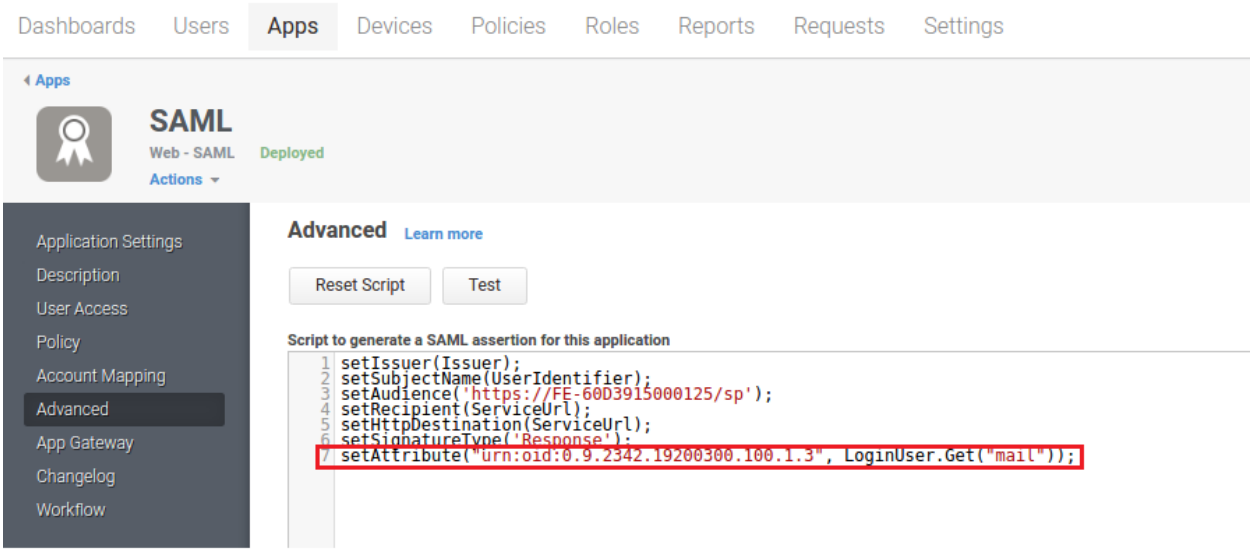
2.4 Copy **Identity Provider SAML Meta data URL** of Centrify to be used later (in step #3.5)



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"));



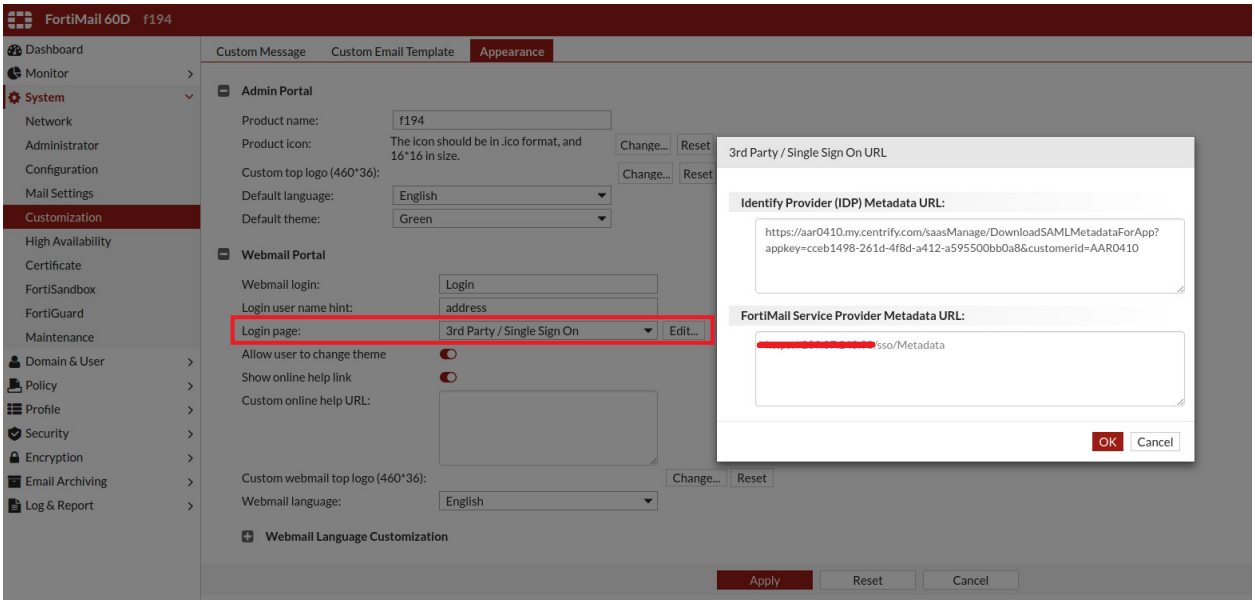
3. How to Enable FortiMail Webmail Single Sign On

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.