RSA SECURID® ACCESS
Implementation Guide

Microsoft Outlook Web Access 2013

RSA Partner Engineering
Last Modified: 11/17/2017

RSA READY

Solution Summary

Microsoft Outlook Web Access (OWA) 2013 is a browser-based email client that lets you access your Microsoft Exchange Server mailbox from almost any web browser. OWA 2013 can be integrated with RSA Cloud Authentication Service as an HFED SSO application.

RSA SecurID Access Features Microsoft Outlook Web Access (OWA) 2013	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	-
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	✓

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

RSA Cloud Authentication Service –Microsoft Outlook Web Access 2013 can be integrated with RSA Cloud Authentication Service in the following way:

HFED SSO

Before You Begin

- Acquire an RSA SecurID Access super administrator account and an OWA end user account.
- Configure DNS canonical names (CNAMES) or aliases for the protected hostnames to the identity router. For example, *exchange2013-exchange-pe-lab-net.sso3.pe-lab.com* is a CNAME to *exchange2013.exchange-pe-lab.net*

Note: You can use a wildcard CNAME to add an HFED application-protected hostname without creating individual DNS entries. For example, **.sso3.pe-lab.com* is a CNAME to *portal.sso3.pe-lab.com.*

- Ask your Microsoft Exchange administrator to verify that your Microsoft Exchange server version is 2013 and that it's running on Window 2008 R2 or later.
- Verify that OWA has been configured to use an SSL certificate that was generated from a trusted Certificate Authority (CA). Self-signed certificates are not supported.

Important: The integration only supports SSL certificates that have been issued by a trusted CA. If your Microsoft Exchange 2013 server has been configured to use a self-signed SSL certificate for OWA client communication, your Microsoft Exchange administrator will need to replace the certificate.

Consult Microsoft Exchange 2013 online documentation more information about configuring SSL for OWA and using a local Microsoft certificate authority, or a third party or commercial certificate authority to generate an SSL certificate:

https://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx

- If your Microsoft Exchange 2013 server uses a local Microsoft CA, or an uncommon third-party or commercial CA for certificate signing, you must upload the CA's root certificate to the IDR. For instructions and a list of CAs the IDR trusts out-of-the-box, see the RSA SecurID Access help documentation.
- Microsoft Exchange connections must use the TLS protocol (RSA highly recommends TLS 1.2) and at least one cipher that is supported by the IDR. Ask your Microsoft Exchange administrator to confirm that your Exchange server meets these requirements. For the current list of supported connection ciphers, see the RSA SecurID Access help documentation. Information about viewing, updating and prioritizing cryptographic protocols and cipher suites for Microsoft Exchange 2013 can be found on Microsoft TechNet . https://technet.microsoft.com.
- Confirm that you can log into your OWA end user account and access you folders, send/receive emails, view your calendar, etc.

Configuration Procedure

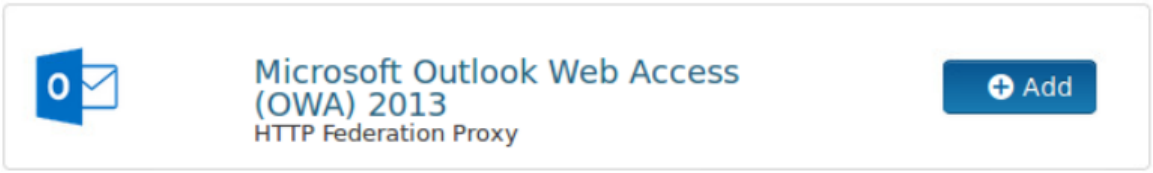
RSA Cloud Authentication Service – Identity Router HFED Configuration
Microsoft Outlook Web Access 2013 HFED Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

1. Log in to the RSA SecurID Access console, click the **Applications** tab and select *Application Catalog* from the **Applications** dropdown list.

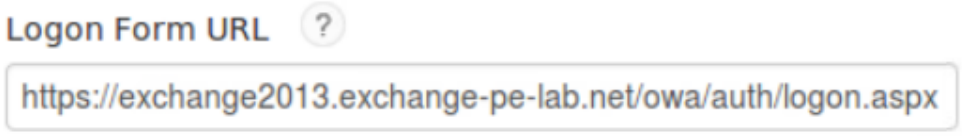
2. Search the list for *Microsoft Outlook Web Access (OWA) 2013* and click the **+Add** button.



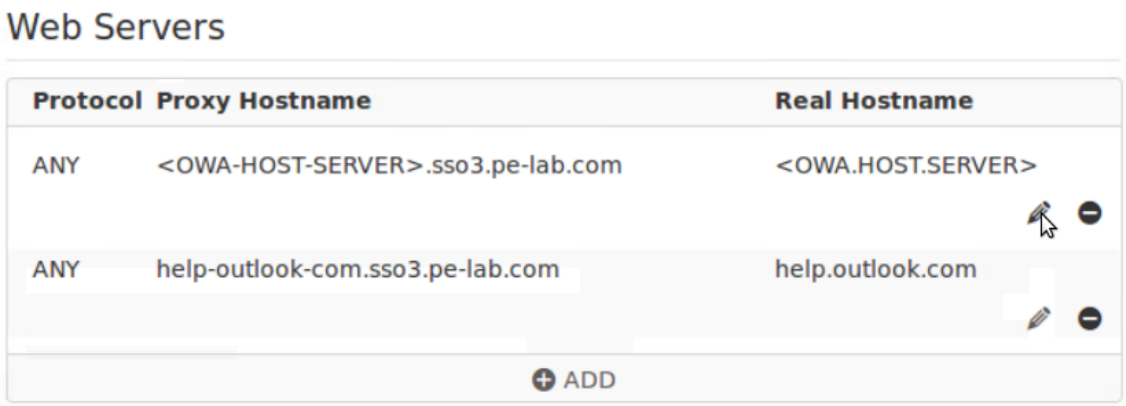
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.
4. When the **Branded Settings** page is displayed, the **Logon Form URL** field will contain a URL with two placeholders variables as illustrated below.

Modify the URL value as follows

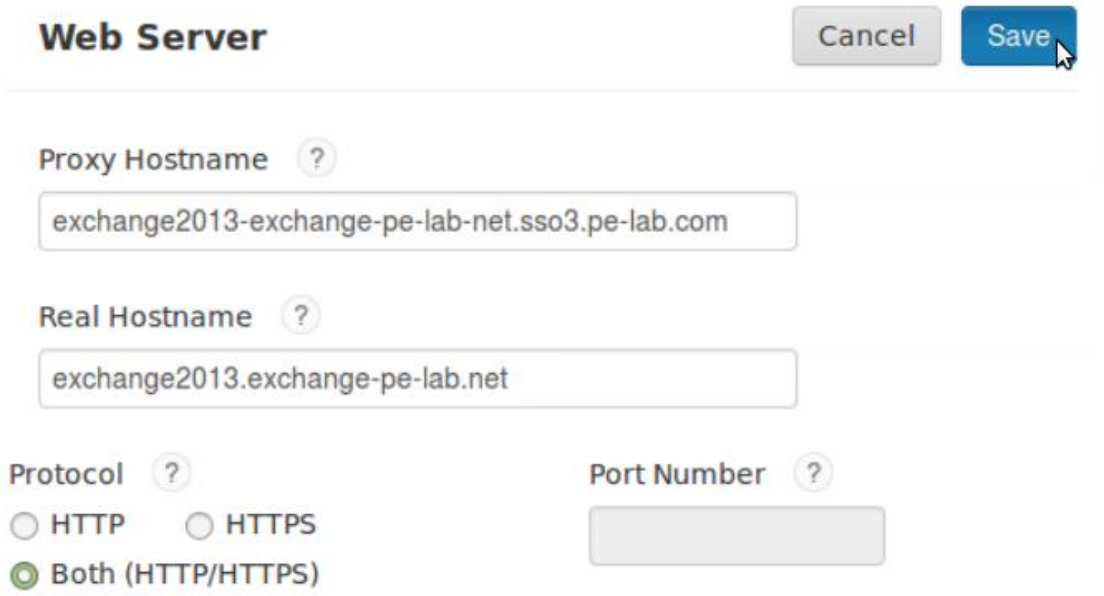
a. Replace the *<OWA.HOST.SERVER>* placeholder with your Microsoft Exchange Server's fully-qualified hostname.
b. Replace the *[:<PORT>]* placeholder with the OWA listening port (preceded by a colon). If OWA is listening on port *443*, simply remove *[:<PORT>]* from the URL. In this example, OWA is listening on 443, so the updated logon form URL would be *https://exchange2013.exchange-pe-lab.net/owa/auth/logon.aspx*.



5. Scroll to the **Web Servers** table and click the pencil icon on the right hand side of the first row.



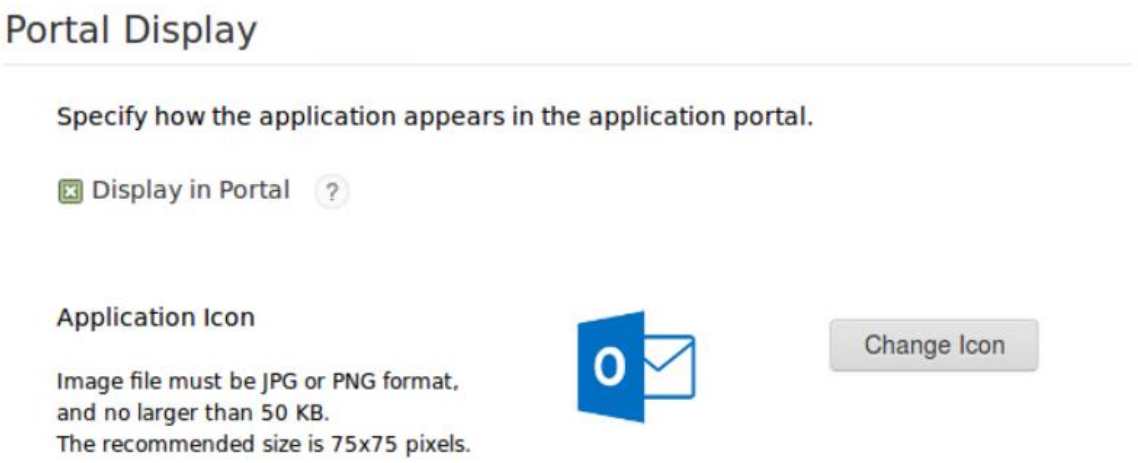
6. Enter the fully-qualified hostname of your proxy web server in the **Proxy Hostname** field. Do not include the internet protocol. Use a valid alias from the DNS database that points to the identity router hostname. For example: *exchange2013-exchange-pe-lab-net.sso3.pe-lab.com*
7. Enter the fully-qualified hostname of your Microsoft Exchange 2013 server in the **Real Hostname** field. Do not include the internet protocol. For example: *exchange2013.exchange-pe-lab.net*
8. If Microsoft Outlook Web Access 2013 is listening on https port 443, you can leave the **Both (HTTP/HTTPS)** radio button selected (default). If it is listening on a different https port, select the **HTTPS** radio button and enter the port number in the **Port Number** field.
9. Click the **Save** button.



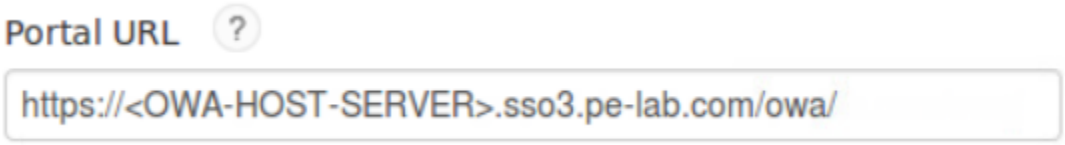
10. Click the **Next Step** button.

11. On the **User Access** page, select the access policy the identity router will use to determine which users can access Microsoft Outlook Web Access 2013 from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise, select the **Select Custom Policy** radio button and select the policy you want to use from the dropdown list.

12. Click the **Next Step** button.
13. Select the **Display in Portal** checkbox on the **Portal Display** page.



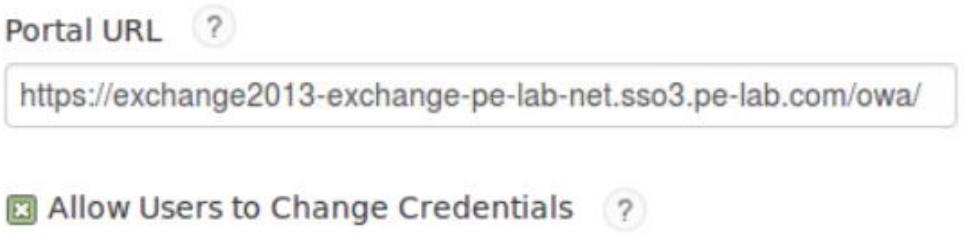
14. The **Portal URL** field will contain a URL with the *<OWA-HOST-SERVER>* placeholder variable as illustrated below:



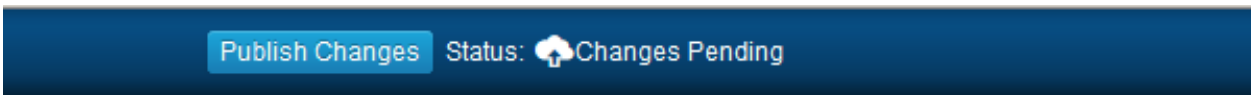
Replace *<OWA-HOST-SERVER>* with the Microsoft Exchange server proxy host portion of your full proxy web server hostname (CNAME). In this example, the host alias is *exchange2013-exchange-pe-lab.net* and the proxy domain is *sso3.pe-lab.com*, so the updated portal URL would be:

https://exchange2013-exchange-pe-lab-net.sso3.pe-lab.com/owa/

15. If you want to allow users to change Oracle EBS credentials after configuring the connector, check **Allow Users to Change Credentials** checkbox



16. Click the **Save and Finish** button.
17. Click the **Publish Changes** button in the top left corner of the page.



Partner Product Configuration

Microsoft Outlook Web Access 2013 HFED Configuration

There are no partner-side configuration changes needed to enable integration with RSA SecurID Access.