

RSA SecurID Access HFED Proxy Configuration for Microsoft Outlook Web Access (OWA)



Last Modified: October 3rd, 2016

Outlook Web App (OWA), originally named Exchange Web Connect and then Outlook Web Access, is a webmail component of Microsoft Exchange Server starting with version 5.0. It is also a part of the Office 365. The Office 365 offering has since been updated to Outlook on the web.

Before You Begin

 **Note:** Before proceeding with this HFED guide, look to see if a SAML guide is available.

- Acquire an administrator account to RSA SecurID Access.
- Verify the RSA SecurID Access user account.
- Configure DNS canonical names (CNAMES), or aliases for the protected hostnames to the identity router. For example:
 - appname.sso.example.com is a CNAME to portal.sso.example.com
 - appname-resources.sso.example.com is a CNAME to portal.sso.example.com

 **Note:** Using a wildcard CNAME you can quickly add HFED application-protected hostnames without creating individual DNS entries. For example:

***.sso.example.com is a CNAME to portal.sso.example.com**

- Acquire an account to Microsoft Outlook Web Access (OWA).

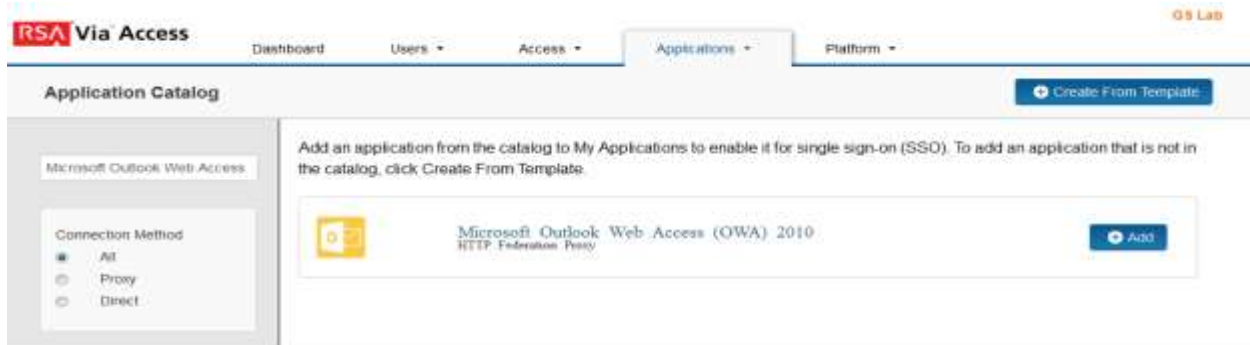
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Microsoft Outlook Web Access \(OWA\) to Use RSA SecurID Access as an Identity Provider](#)

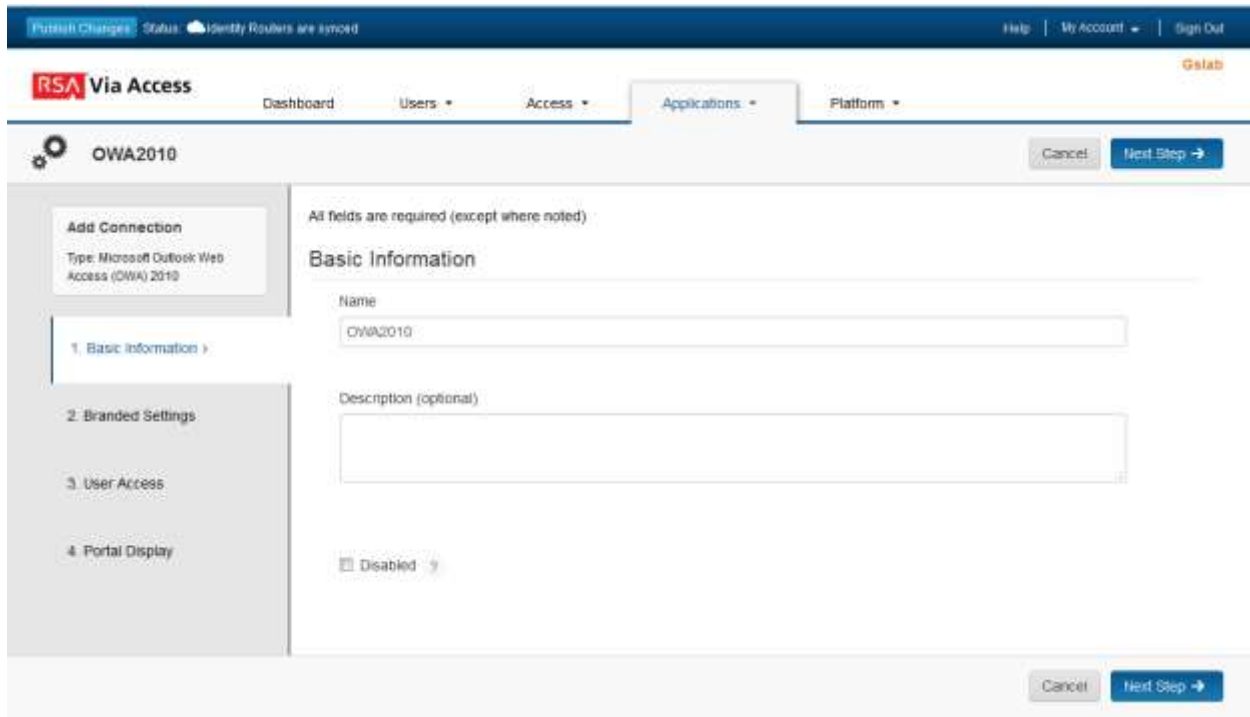
Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, select **Microsoft Outlook Web Access (OWA) HTTP Federation Proxy** and click **+Add**.



3. On the Basic Information page, specify the application name and click **Next Step**.



4. On the Branded Settings page, verify the **Logon Form URL**.
5. Click on **Next Step**.

The screenshot shows the RSA Via Access interface for configuring an OWA2010 application. The top navigation bar includes 'Push Changes', 'Status: Identity Routers are synced', 'Help', 'My Account', and 'Sign Out'. The main navigation has 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The left sidebar shows 'Add Connection' (Type: Microsoft Outlook Web Access (OWA) 2010) and a list of steps: '1. Basic Information', '2. Branded Settings >', '3. User Access', and '4. Portal Display'. The main content area is titled 'Branded Settings' and includes a note: 'All fields are required (except where noted)'. The 'Logon Form URL' field contains 'https://<OWA2010_SERVER>/owa/auth/logon.aspx'. Below this are checkboxes for 'Pass Attributes', 'Pass Headers', and 'Verify Certificates'. The 'Web Servers' section contains a table with two entries:

Protocol	Proxy Hostname	Real Hostname	
ANY	<OWA2010_SERVER> gslab.com	<OWA2010_SERVER>	
ANY	help.outlook.com gslab.com	help.outlook.com	

An 'ADD' button is located at the bottom of the table. 'Cancel' and 'Next Step' buttons are visible in the top right corner.

6. On the User Access page, choose **Allow All Authenticated Users**. Click on **Next Step**.

The screenshot shows the RSA Via Access interface for configuring the User Access for the OWA2010 application. The top navigation bar and main navigation are the same as in the previous screenshot. The left sidebar shows the same 'Add Connection' and step list, with '3. User Access >' highlighted. The main content area is titled 'User Access' and includes a note: 'All fields are required (except where noted)'. It prompts the user to 'Select the access policy to determine which users are allowed to access the application'. Two radio button options are present: 'Allow All Authenticated Users' (which is selected) and 'Select Custom Policy'. Below the radio buttons is a dropdown menu currently set to 'No Access Allowed'. 'Cancel' and 'Next Step' buttons are visible in the top right corner.

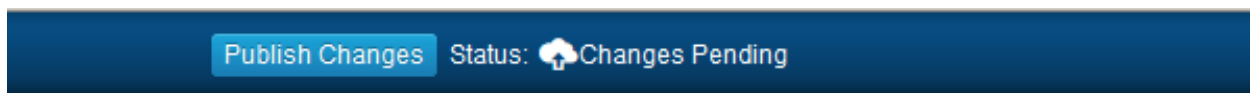
7. On the Portal Display page, check **Display in Portal** checkbox.
8. Check if the Application icon is displayed. Else click **Change Icon** and browse for the image on your local machine.
9. If you want to allow users to change the credentials after configuring connector, then check **Allow Users to Change Credentials**.

The screenshot shows the 'Portal Display' configuration page for an OWA connection. The page title is 'OWA' and it includes 'Cancel' and 'Save and Finish' buttons at the top right. A sidebar on the left lists navigation options: 'Add Connection', '1. Basic Information', '2. Branded Settings', '3. User Access', and '4. Portal Display >'. The main content area is titled 'Portal Display' and contains the following fields and options:

- A note: 'All fields are required (except where noted)'
- Section: 'Specify how the application appears in the end-user portal'
- Checkbox: Display in Portal
- Section: 'Application Icon'
- Image: A yellow square icon with a white 'O' and a mail symbol.
- Text: 'Image file must be JPG or PNG format, and no larger than 50 KB. The recommended size is 75x75 pixels.'
- Button: 'Change Icon'
- Text: 'Application Tooltip' with input field containing 'OWA2010'
- Text: 'Portal URL' with input field containing 'https://login.microsoftonline.com/gslab.com/owa/'
- Checkbox: Allow Users to Change Credentials

'Cancel' and 'Save and Finish' buttons are also present at the bottom right of the configuration area.

10. Click **Save and Finish**.
11. Click **Publish Changes**.



Configure Microsoft Outlook Web Access (OWA) to Use RSA SecurID Access as an Identity Provider

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