

How to configure the UTM Web Application Firewall for Microsoft Exchange connectivity

This article explains how to configure your Sophos UTM to allow access to the relevant Microsoft Exchange services through the Web Application Firewall.

Configuring your Exchange server is outside the scope of this guide; This article assumes you've already setup your Microsoft Exchange environment for remote connectivity and that you have copies of your SSL certificates available in PFX format.

Known to apply to the following Sophos product(s) and version(s)
Sophos UTM 9.1

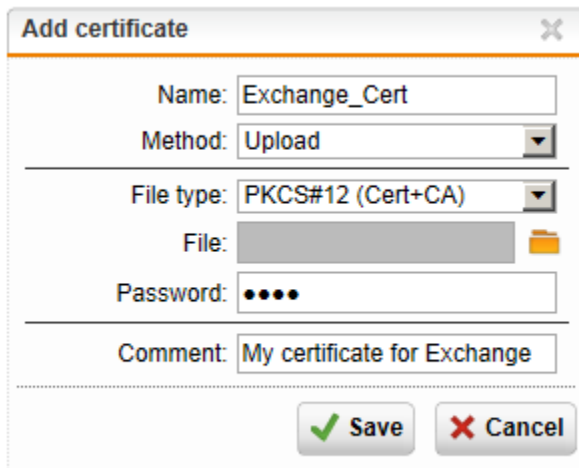
Operating systems

Microsoft Windows Server 2003 – 2012, Microsoft Exchange 2007-2013

What To Do

A. Import the required certificates

1. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Certificate Management"
2. Click "New Certificate" and select "Upload" in the "Method:" dropdown box

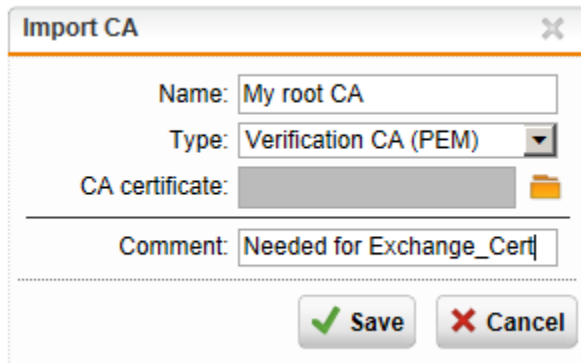


3. Fill in a name, the required password and a comment (if needed)
4. Click the folder next to the upload field to select the PFX file you wish to import
5. Click "save" to upload the PFX and complete the import

B. Optional: Import the root Certificate

In case your PFX file does not include the root certificate you need to manually import it in order for the UTM to be able to use it.

1. Go to certificate management and navigate to the "Certificate Authority" tab.
2. Click the "Import CA" button and fill in the name, description and type (this should usually be "Verification CA")



The screenshot shows a dialog box titled "Import CA". It contains the following fields and controls:

- Name:** A text input field containing "My root CA".
- Type:** A dropdown menu currently showing "Verification CA (PEM)".
- CA certificate:** A text input field that is currently empty, followed by a folder icon button for file selection.
- Comment:** A text input field containing "Needed for Exchange_Cert".
- Buttons:** At the bottom, there are two buttons: "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

3. Click the folder next to the upload field to select the certificate to upload (both PFX and CER format are supported)
4. Click save to upload the certificate and complete the import

C. Configuring the firewall profiles

Exchange contains several web services (Outlook Anywhere, Outlook Web App (OWA), Exchange ActiveSync and Exchange Autodiscover) which require different levels of protection. As a result of this, you need to configure separate profiles for each service.

The profile options configured below are based on our recommended settings and the items marked (Optional) should be treated as our personal suggestions.

Outlook Web App (OWA)

1. Go to the “Webserver Protection” menu in the UTM Web admin console and select “Web Application Firewall”
2. Navigate to the “Firewall Profiles” tab and click the “New Firewall Profile” button
3. Fill in a Name for the profile and select the appropriate firewall action (Drop, Reject or Accept) from the “Mode:” dropdown menu (Monitor logs the traffic and allows it, Reject drops the traffic and informs the end user's browser, Drop silently drops the traffic)
4. Enable the Cross Site Scripting (XSS) and SQL Injection Filters
5. Enable URL Hardening and enter “/owa” and “/OWA” as entry points by clicking the “+” icon in the top right corner of the checkbox.
6. (Optional) Enable antivirus scanning, select the engine mode (Single or Dual engine) and Scan mode (Upload, Download or Upload and Download) from the dropdown menu's
7. (Optional) Block suspect hosts by enabling the “Block clients with bad reputation” feature
8. Click the “Save” button to store the profile and continue

The following screenshot displays our recommended settings:

Edit Firewall Profile

Name:

☐ Pass Outlook Anywhere

Mode:

☒ Cross Site Scripting (XSS) Filter

☒ SQL Injection Filter

☐ Cookie signing

☒ URL Hardening

Entry URLs

Entry URLs

+

...

▼

☐ Form Hardening

☒ Antivirus scanning

AV Engines:

Scan

☐ Block unscannable content

☒ Block clients with bad reputation

Comment:

+
Advanced profile settings

✓ Save

✗ Cancel

Exchange Autodiscover

9. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
10. Navigate to the "Firewall Profiles" tab and click the "New Firewall Profile" button
11. Fill in a Name for the profile and select the appropriate firewall action (Drop, Reject or Accept) from the "Mode:" dropdown menu
12. Enable the SQL Injection Filter
13. Enable URL Hardening and enter "/autodiscover" and "/Autodiscover" as entry points by clicking the "+" icon in the top right corner of the checkbox.
14. (Optional) Enable antivirus scanning, select the engine mode (Single or Dual engine) and Scan mode (Upload, Download or Upload and Download) from the dropdown menu's
15. (Optional) Block suspect hosts by enabling the "Block clients with bad reputation" feature
16. Click "Save" to store the profile and continue

The following screenshot displays our recommended settings:

The screenshot shows the 'Edit Firewall Profile' dialog box with the following settings:

- Name: Exchange Autodiscover
- ☐ Pass Outlook Anywhere
- Mode: drop
- ☐ Cross Site Scripting (XSS) Filter
- ☒ SQL Injection Filter
- ☐ Cookie signing
- ☒ URL Hardening
- Entry URLs: specified manually
- Entry URLs list:
 - /autodiscover
 - /Autodiscover
- ☒ Form Hardening
- ☐ Antivirus scanning
- ☒ Block clients with bad reputation
- Comment: (empty)
- Advanced profile settings (expanded)

Buttons: Save, Cancel

Exchange ActiveSync

17. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
18. Navigate to the "Firewall Profiles" tab and click the "New Firewall Profile" button
19. Fill in a Name for the profile and select the appropriate firewall action (Drop, Reject or Accept) from the "Mode:" dropdown menu
20. Enable the SQL Injection Filter
21. Enable URL Hardening and enter "/Exchange-Server-ActiveSync" and "/exchange-server-activesync" as entry points by clicking the "+" icon in the top right corner of the checkbox.
22. (Optional) Enable antivirus scanning, select the engine mode (Single or Dual engine) and Scan mode (Upload, Download or Upload and Download) from the dropdown menu's
23. (Optional) Block suspect hosts by enabling the "Block clients with bad reputation" feature
24. Click "Save" to store the profile and continue

The following screenshot displays our recommended settings

The screenshot shows the 'Edit Firewall Profile' window with the following settings:

- Name:** Exchange ActiveSync
- ☐ Pass Outlook Anywhere
- Mode:** drop
- ☐ Cross Site Scripting (XSS) Filter
- ☒ SQL Injection Filter
- ☐ Cookie signing
- ☒ URL Hardening
- Entry URLs:** specified manually
- Entry URLs list:**
 - /Microsoft-Server-ActiveSync
 - /microsoft-server-activesync
- ☐ Form Hardening
- ☒ Antivirus scanning
- AV Engines:** Dual Scan
- Scan:** Uploads and Downloads
- ☐ Block unscannable content
- ☒ Block clients with bad reputation
- Comment:** (empty)
- Advanced profile settings:** (expanded)

At the bottom are 'Save' and 'Cancel' buttons.

Outlook Anywhere

1. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
2. Navigate to the "Firewall Profiles" tab and click the "New Firewall Profile" button
3. Fill in a Name for the profile and select the appropriate firewall action (Drop, Reject or Accept) from the "Mode:" dropdown menu
4. Enable the "Pass Outlook Anywhere" option
5. Enable URL Hardening and enter "/rpc", "/RPC", "/oab", "/OAB", "/ews" and "/EWS" as entry points by clicking the "+" icon in the top right corner of the checkbox.
6. (Optional) Block suspect hosts by enabling the "Block clients with bad reputation" feature
7. Click "Save" to store the profile and continue

The following screenshot displays our recommended settings:

Edit Firewall Profile

Name: Outlook Anywhere

☒ Pass Outlook Anywhere

Mode: drop

☐ Cross Site Scripting (XSS) Filter

☐ SQL Injection Filter

☐ Cookie signing

☒ URL Hardening

Entry URLs specified manually

Entry URLs

/rpc
/ews
/osb
/RPC
/EWS

☐ Form Hardening

☐ Antivirus scanning

☒ Block clients with bad reputation

Comment:

+ Advanced profile settings

Save
Cancel

D. Creating the Real Webserver(s)

Outlook Web App (OWA)

1. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
2. Navigate to the "Real Webserver" tab and click the "New Real Webserver" button
3. Fill in a Name for the new Real Webserver and select either a pre-existing Host object by clicking the folder icon or create one by clicking the "+" button

Edit Real Webserver

Name:

Host: Internal mail server

Type: SSL (HTTPS)

Port:

Comment:

Advanced settings

Save Cancel

4. Set the Real Webserver connection type by selecting either “HTTP” or “HTTPS” from the “Type” dropdown menu.
5. (Optional) After selecting the appropriate connection type the UTM will automatically fill in the associated port, should you however need to use a non-standard port you can enter it in the “Port” field.

Repeat the above procedure for every Exchange server in your farm. For the rest of this guide we are going to assume a minimum of two servers, but the configuration for a single server is practically similar.

E. Creating the Virtual Webservers

Since we intend to use different firewall profiles for different Exchange services (as previously discussed) we will need to configure a matching amount of Virtual Webservers to which these profiles should apply.

Outlook Web App (OWA)

1. Go to the “Webserver Protection” menu in the UTM Web admin console and select “Web Application Firewall”
2. Navigate to the “Virtual Webservers” tab and click the “New Virtual Webserver” button
3. Fill in a Name for the Virtual server
4. Select the interface on which this Virtual Webserver should be created from the “Interface” dropdown menu, along with the protocol the end-users should use to connect to this server from the “Type” menu. For the intents and purposes of this article – securely enabling remote access to your Exchange environment) we will set this to HTTPS.
5. (Optional) The UTM will automatically fill in the standard port associated to the HTTPS protocol, but you can set an alternate port in the “Port:” field.
6. Select the applicable certificate from the “Certificate:” dropdown menu
7. Select either the desired domain name from the “Domains:” list, or (when using a wildcard certificate) enter your desired hostname by clicking the “+” button in the top right corner. (Sophos advises you to use a SAN certificate here, as wildcard certificates are incompatible with multi-site High Availability (HA) Exchange setups and require extra configuration on the Exchange server(s))
8. Select the Firewall Profile you’ve created for the Exchange OWA from the “Firewall Profile” dropdown menu
9. Enable the “Pass Host Header” option (**this is very important as your Exchange server needs the actual host header to determine the location (inside/outside the organization) of the client, on which many Exchange services rely**)
10. Click the “Save” button to store the configuration and continue

The following screenshot displays our recommended settings:

Edit Virtual Webserver

Name:

Interface:

Type:

Port:

Certificate:

Domains:

- ☒ webmail.example.com
- ☐ oa.example.com
- ☐ autodiscover.example.com

Real Webservers:

- ☒ Exchange #1 *enabled*
- ☒ Exchange #2 *enabled*
- ☐ Lync Frontend #1 - HTTP *enabled*
- ☐ Lync Frontend #1 - HTTPS *enabled*

Firewall Profile:

☐ Enable HTML rewriting

☒ Pass Host Header

☐ Disable compression support

Comment:

Exchange Autodiscover

As part of Microsoft's best practices Sophos recommends running the Autodiscover service on a separate hostname. This hostname should normally be autodiscover.<domain>.<tld>, as demonstrated below.

11. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
12. Navigate to the "Virtual Webservers" tab and click the "New Virtual Webserver" button
13. Fill in a Name for the Virtual server
14. Select the interface on which this Virtual Webserver should be created from the "Interface" dropdown menu, along with the protocol the end-users should use to connect to this server from

the “Type” menu. For the intents and purposes of this article – securely enabling remote access to your Exchange environment) we will set this to HTTPS.

15. (Optional) The UTM will automatically fill in the standard port associated to the HTTPS protocol, but you can set an alternate port in the “Port:” field.
16. Select the applicable certificate from the “Certificate:” dropdown menu
17. Select either the desired domain name from the “Domains:” list, or (when using a wildcard certificate) enter your desired hostname by clicking the “+” button in the top right corner.
18. Select the Firewall Profile you’ve created for Exchange Autodiscover from the “Firewall Profile” dropdown menu
19. Enable the “Pass Host Header” option (**failure to set this option will break automatic configuration for all Exchange ActiveSync and Outlook Anywhere clients, as well as automatic failover in HA scenario’s**)
20. Click the “Save” button to store the configuration and continue

The following screenshot displays our recommended settings:

The screenshot shows the 'Edit Virtual Webserver' configuration window. The settings are as follows:

- Name:** Autodiscover
- Interface:** External (WAN) (Address)
- Type:** SSL (HTTPS)
- Port:** 443
- Certificate:** Webmail
- Domains:**
 - ☐ webmail.example.com
 - ☐ oa.example.com
 - ☒ autodiscover.example.com
- Real Webservers:**
 - ☒ Exchange #1 *enabled*
 - ☒ Exchange #2 *enabled*
 - ☐ Lync Frontend #1 - HTTP *enabled*
 - ☐ Lync Frontend #1 - HTTPS *enabled*
- Firewall Profile:** Exchange Autodiscover
- ☐ Enable HTML rewriting
- ☒ Pass Host Header
- ☐ Disable compression support
- Comment:** (empty field)

At the bottom, there are two buttons: a green 'Save' button and a red 'Cancel' button.

Exchange ActiveSync

21. Go to the “Webserver Protection” menu in the UTM Web admin console and select “Web Application Firewall”
22. Navigate to the “Virtual Webserver” tab and click the “New Virtual Webserver” button
23. Fill in a Name for the Virtual server
24. Select the interface on which this Virtual Webserver should be created from the “Interface” dropdown menu, along with the protocol the end-users should use to connect to this server from the “Type” menu. For the intents and purposes of this article – securely enabling remote access to your Exchange environment) we will set this to HTTPS.
25. (Optional) The UTM will automatically fill in the standard port associated to the HTTPS protocol, but you can set an alternate port in the “Port:” field.
26. Select the applicable certificate from the “Certificate:” dropdown menu
27. Select either the desired domain name from the “Domains:” list, or (when using a wildcard certificate) enter your desired hostname by clicking the “+” button in the top right corner.
28. Select the Firewall Profile you’ve created for Exchange ActiveSync from the “Firewall Profile” dropdown menu
29. Enable the “Pass Host Header” option (**Exchange determines the applicable automatic configuration (received through Autodiscover) based on the host header used to connect to ActiveSync, this option is therefore very important**)
30. Click the “Save” button to store the configuration and continue

The following screenshot displays our recommended settings:

✕

Edit Virtual Webserver

Name: Exchange ActiveSync

Interface: External (WAN) (Address)

Type: SSL (HTTPS)

Port: 443

Certificate: Webmail

Domains:

☐ webmail.example.com
☐ oa.example.com
☐ autodiscover.example.com
☒ activesync.example.com

Real Webservers:

☒ Exchange #1 enabled
☒ Exchange #2 enabled
☐ Lync Frontend #1 - HTTP enabled
☐ Lync Frontend #1 - HTTPS enabled

Firewall Profile: Exchange ActiveSync

☐ Enable HTML rewriting
☒ Pass Host Header
☐ Disable compression support

Comment:

✓ Save

✕ Cancel

Please note: If you've deployed both Exchange OWA and ActiveSync on the same hostname on the Exchange servers you will run into a problem trying to activate this Virtual Webserver. A solution to this issue is provided below, in step F.

Outlook Anywhere

As outlined in our configuration instructions and screenshot below we've configured Outlook Anywhere to operate on a different hostname from OWA and the other Exchange services. This is due to the fact that enabling "pass Outlook Anywhere" is incompatible with the traffic generated by other Exchange services such as OWA. Please be aware of this when setting up your UTM.

31. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
32. Navigate to the "Virtual Webservers" tab and click the "New Virtual Webserver" button
33. Fill in a Name for the Virtual server
34. Select the interface on which this Virtual Webserver should be created from the "Interface" dropdown menu, along with the protocol the end-users should use to connect to this server from

the “Type” menu. For the intents and purposes of this article – securely enabling remote access to your Exchange environment) we will set this to HTTPS.

35. (Optional) The UTM will automatically fill in the standard port associated to the HTTPS protocol, but you can set an alternate port in the “Port:” field.
36. Select the applicable certificate from the “Certificate:” dropdown menu
37. Select either the desired domain name from the “Domains:” list, or (when using a wildcard certificate) enter your desired hostname by clicking the “+” button in the top right corner.
38. Select the Firewall Profile you’ve created for Outlook Anywhere from the “Firewall Profile” dropdown menu
39. Enable the “Pass Host Header” option (**Outlook Anywhere compares the certificate used in the connection with the hostname configured on the Exchange server(s). Any connection using Outlook Anywhere will fail if these do not match. Setting this option is therefore very important**)
40. Click the “Save” button to store the configuration and continue

The following screenshot displays our recommended settings:

The screenshot shows the 'Edit Virtual Webserver' configuration window. The settings are as follows:

- Name:** Outlook Anywhere
- Interface:** External (WAN) (Address)
- Type:** SSL (HTTPS)
- Port:** 443
- Certificate:** Webmail
- Domains:**
 - ☐ webmail.example.com
 - ☒ oa.example.com
 - ☐ autodiscover.example.com
- Real Webservers:**
 - ☒ Exchange #1 *enabled*
 - ☒ Exchange #2 *enabled*
 - ☐ Lync Frontend #1 - HTTP *enabled*
 - ☐ Lync Frontend #1 - HTTPS *enabled*
- Firewall Profile:** Outlook Anywhere
- ☐ Enable HTML rewriting
- ☒ Pass Host Header
- ☐ Disable compression support
- Comment:** (empty text box)

At the bottom, there are two buttons: a green 'Save' button and a red 'Cancel' button.

F. **Configuring Exceptions**

Since the URL Filtering feature in UTM is very strict, it will currently not allow clients to open any URL other than the ones we've configured. This means that "webmail.example.com/owa" is allowed, but "webmail.example.com/owa/auth/login.aspx" or "webmail.example.com/owa/directory/anything" will be dropped.

To enable the clients to access these virtual directories, you need to create an Exception to allow for a little less stringent filtering.

Outlook Web App (OWA)

1. Navigate to the "Exceptions" tab and click the "New Exception" button
2. Set a Name for the exception and (if needed) Write a description in the "Comment:" field
3. Enable the "URL Hardening" option in the "Skip these checks" menu
4. Select your Exchange OWA Virtual Webserver from the "On the virtual server" dropdown menu
5. Set the "For all requests" dropdown menu to "Web requests matching this path"
6. Click the "+" button in the top right corner to create the a new excepted path and enter "/owa/*" and "/OWA/*".
7. Click the "Save" button to store the configuration and continue.

The following screenshot displays our recommended settings for the exception:

✕

Name: Exchange OWA

Comment:

Skip these checks

☐ SQL Injection Filter

☐ Cross Site Scripting (XSS) Filter

☐ Cookie Signing

☒ URL Hardening

☐ Form Hardening

☐ Antivirus

☐ Block clients with bad reputation

On the virtual webserver

OWA

For all requests

Web requests matching this path

⌵

✕ Delete

Paths

+

⋮

⌵

🗑

/owa/*

🗑

/OWA/*

and

⌵

 :: Please select ::

⌵

+

 Advanced

✓ Save

✕ Cancel

Exchange Autodiscover

8. Navigate to the “Exceptions” tab and click the “New Exception” button
9. Set a Name for the exception and (if needed) Write a description in the “Comment:” field
10. Enable the “URL Hardening” option in the “Skip these checks” menu
11. Select your Exchange Autodiscover Virtual Webserver from the “On the virtual server” dropdown menu
12. Set the “For all requests” dropdown menu to “Web requests matching this path”
13. Click the “+” button in the top right corner to create the a new excepted path and enter “/autodiscover/*” and “/Autodiscover/*”
14. Click the “Save” button to store the configuration and continue.

The following screenshot displays our recommended settings for the exception:

✕

Edit Exception List

Name:

Exchange Autodiscover

Comment:

Skip these checks

☐ SQL Injection Filter

☐ Cross Site Scripting (XSS) Filter

☐ Cookie Signing

☒ URL Hardening

☐ Form Hardening

☐ Antivirus

☐ Block clients with bad reputation

On the virtual webserver


Exchange Autodiscover


For all requests

Web requests matching this path

✕ Delete

Paths

 /autodiscover/*

 /Autodiscover/*

and

:: Please select ::

+ Advanced

✓ Save

✕ Cancel

Exchange ActiveSync

If your ActiveSync is sharing the hostname with your OWA profile, please skip these instructions and continue at step 22.

15. Navigate to the “Exceptions” tab and click the “New Exception” button
16. Set a Name for the exception and (if needed) Write a description in the “Comment:” field
17. Enable the “URL Hardening” option in the “Skip these checks” menu
18. Select your Exchange ActiveSync Virtual Webserver from the “On the virtual server” dropdown menu
19. Set the “For all requests” dropdown menu to “Web requests matching this path”
20. Click the “+” button in the top right corner to create the a new excepted path and enter “/Microsoft-Server-ActiveSync/*” and “/Microsoft-server-activesync/*”
21. Click the “Save” button to store the configuration and continue.

The following screenshot displays our recommended settings for the exception:

The screenshot shows the 'Edit Exception List' window with the following settings:

- Name:** Exchange ActiveSync
- Comment:** (empty)
- Skip these checks:**
 - ☐ SQL Injection Filter
 - ☐ Cross Site Scripting (XSS) Filter
 - ☐ Cookie Signing
 - ☒ URL Hardening
 - ☐ Form Hardening
 - ☐ Antivirus
 - ☐ Block clients with bad reputation
- On the virtual webserver:** ActiveSync
- For all requests:** Web requests matching this path (with a dropdown arrow) and a 'Delete' button.
- Paths:** A list containing two entries: /Microsoft-Server-ActiveSync/* and /microsoft-server-activesync/*.
- and:** A dropdown menu currently showing 'Please select ::'.
- Advanced:** A section with a '+' icon and the word 'Advanced'.
- Buttons:** 'Save' (with a green checkmark) and 'Cancel' (with a red X).

Exchange ActiveSync (Only when sharing FQDN)

As previously mentioned, those trying to enable both Exchange ActiveSync and OWA on the same IP address and hostname will be unable to activate both profiles simultaneously.

The UTM will, upon trying to enable the rule, inform you that another profile using this same combination of hostname and IP address is already active.

To work around this behavior we will have to slightly modify the Firewall Profile used by either OWA or ActiveSync (we'll use OWA in this example) and create an Exception in the WAF.

22. Go to the "Webserver Protection" menu in the UTM Web admin console and select "Web Application Firewall"
23. Navigate to the "Firewall Profiles" tab, select the Exchange OWA profile and click the "edit" button

24. Change the "URL Hardening" list to include "/Microsoft-Server-ActiveSync" and "/microsoft-server-activesync"
25. Click "Save" to store the alterations and continue
26. Navigate to the "Exceptions" tab and click the "New Exception" button
27. Set a Name for the exception and (if needed) Write a description in the "Comment:" field
28. Enable the "Cross Site Scripting (XSS) Filter" and "URL Hardening" checkboxes in the "Skip these checks" menu
29. Select your OWA Virtual Webserver from the "On the virtual server" dropdown menu
30. Set the "For all requests" dropdown menu to "Web requests matching this path"
31. Click the "+" button in the top right corner to create the excepted path and enter "/Microsoft-Server-ActiveSync/*" and "/microsoft-server-activesync/*".
32. Click the "Save" button to store the configuration and continue.

The following screenshot displays our recommended settings for the exception:

The screenshot shows the 'Edit Exception List' dialog box with the following configuration:

- Name:** Exchange ActiveSync
- Comment:** (Empty field)
- Skip these checks:**
 - ☐ SQL Injection Filter
 - ☒ Cross Site Scripting (XSS) Filter
 - ☐ Cookie Signing
 - ☒ URL Hardening
 - ☐ Form Hardening
 - ☐ Antivirus
 - ☐ Block clients with bad reputation
- On the virtual webserver:** OWA
- For all requests:** Web requests matching this path (with a 'Delete' button)
- Paths:**
 - /Microsoft-Server-ActiveSync/*
 - /microsoft-server-activesync/*
- and:** :: Please select ::
- Advanced:** (Expanded section)
- Buttons:** Save (green checkmark) and Cancel (red X)

Exchange Outlook Anywhere

33. Navigate to the “Exceptions” tab and click the “New Exception” button
34. Set a Name for the exception and (if needed) Write a description in the “Comment:” field
35. Enable the “URL Hardening” option in the “Skip these checks” menu
36. Select your Exchange Outlook Anywhere Virtual Webserver from the “On the virtual server” dropdown menu
37. Set the “For all requests” dropdown menu to “Web requests matching this path”
38. Click the “+” button in the top right corner to create the a new excepted path and enter “/rpc/*”
39. Repeat the previous steps for “/RPC/*”, “/ews/*”, “/EWS/*”, “/oab/*” and “/OAB/*”
40. Click the “Save” button to store the configuration and finish this guide.

The following screenshot displays our recommended settings for the exception:

The screenshot shows the 'Edit Exception List' dialog box with the following configuration:

- Name:** Exchange Outlook Anywhere
- Comment:** (Empty field)
- Skip these checks:**
 - ☐ SQL Injection Filter
 - ☐ Cross Site Scripting (XSS) Filter
 - ☐ Cookie Signing
 - ☒ URL Hardening
 - ☐ Form Hardening
 - ☐ Antivirus
 - ☐ Block clients with bad reputation
- On the virtual webserver:** Exchange Outlook Anywhere
- For all requests:** Web requests matching this path (with a 'Delete' button)
- Paths:** A list containing /rpc/*, /ews/*, /oab/*, /RPC/*, and /EWS/*.
- and:** :: Please select ::
- Advanced:** (Expanded section)
- Buttons:** Save (green checkmark) and Cancel (red X).