

Protecting OWA and ActiveSync with FortiWeb

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



Securing ActiveSync with FortiWeb

Updated on March 17, 2020

TABLE OF CONTENTS

Overview	4
Securing OWA with FortiWeb	7
FortiWeb configuration	8
Step 1 - LDAP query	8
Step 2 - Authentication server pool	8
Step 3 - Site publish rule	9
Step 4 - Site publish policy	10
Step 5 - X-Forwarded-For rule	10
Step 6 - Web protection profile	11
Step 7 - Virtual server	12
Step 8 - Server pool	12
Step 9 - Certificates	12
Step 10 - Server policy	12
LDAP query best practices and tips	13
Outlook Web App configuration	14
Securing ActiveSync with FortiWeb	16
Use Case 1: Scanning ActiveSync Email Attachments	16
Exchange 2010	16
Exchange 2013/2016/2019	17
FortiWeb Configuration	18
Use Case 2: Managing Authentication and SSO to ActiveSync	21
Exchange 2010	22
Exchange 2013/2016/2019	23
FortiWeb Configuration	24

Overview

ActiveSync is a Microsoft technology that has brought data synchronization and server access to hundreds of millions of mobile devices since its introduction. In over 20 years it has evolved to be the foundation of mobile access to today's latest email and server products, including Microsoft Exchange, Office 365, and IBM Notes. Chances are you're using ActiveSync if your organization uses Microsoft Exchange and you're accessing your email on an iOS, Android, Windows Mobile, or BlackBerry device.

Along with ActiveSync, Outlook on the Web is the standard for browser based access to Exchange and Office 365 for email, contacts, tasks, and other services managed by these servers. Outlook for the Web has had many previous names including Exchange Web Connect, Outlook Web Access, and Outlook Web App. Most people know it as OWA for Outlook Web Access. Both ActiveSync and OWA are widely used; however, they present a security challenge to IT teams, as the data sent from a mobile device or a web browser could bypass traditional threat detection systems in certain situations.

The security loophole with ActiveSync and OWA

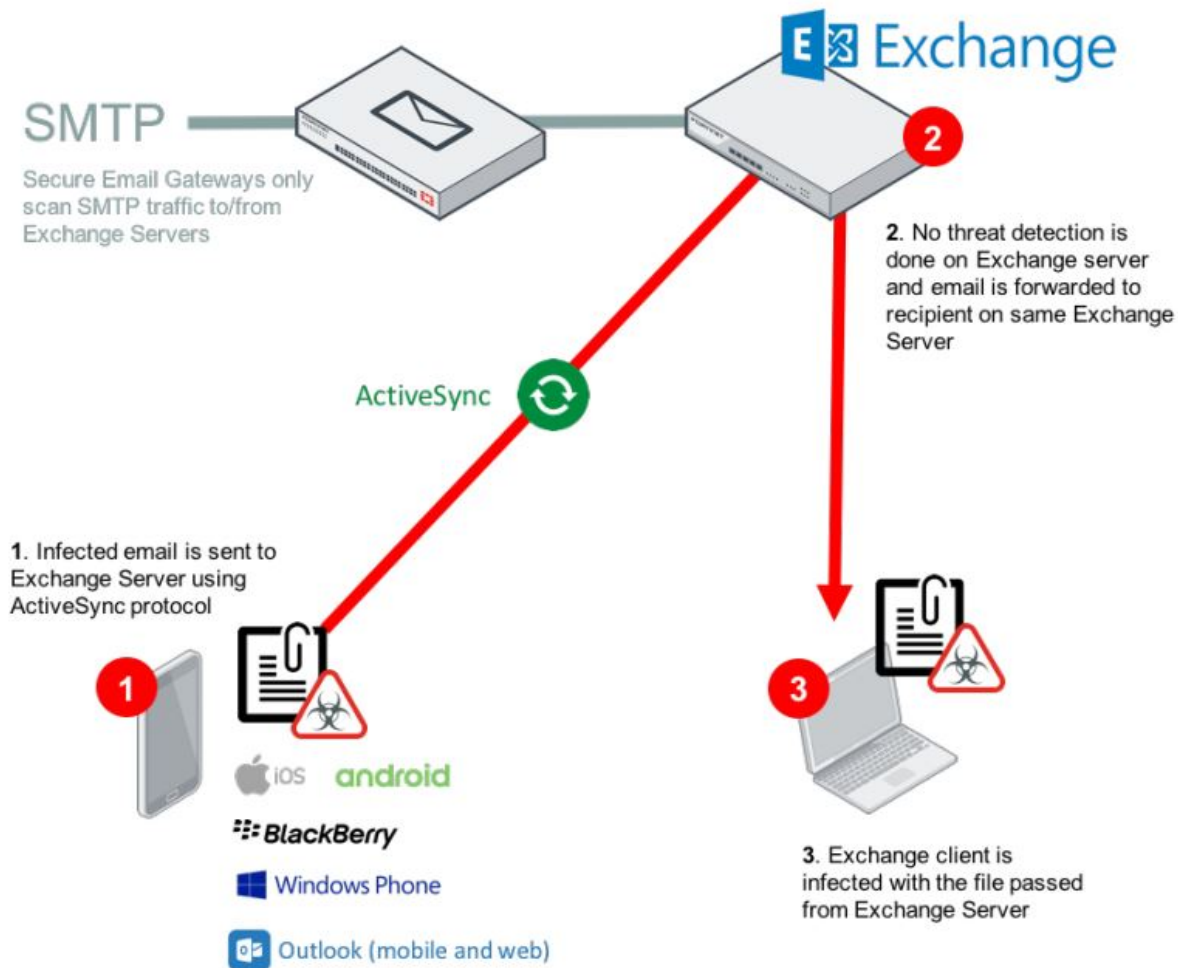
When remote users send and receive emails using ActiveSync or OWA, the server directly communicates with the devices, bypassing email protection services that scan SMTP traffic. Secure Email Gateways (SEGs) only scan inbound and outbound emails from users that are external to the communications server using SMTP.

The ActiveSync protocol is based on XML and uses HTTPS to communicate to the server. OWA is a browser-based method that communicates to the server using HTTP and HTTPS. SEGs have no visibility to this traffic and can't intercept threats that may be hidden inside.

Using Microsoft Exchange as an example, if a remote user sends an email infected with malware using their mobile device or OWA to a recipient outside the organization's Exchange Server, the email would be flagged and acted upon by the SEG. However, recipients on the same Exchange Server as the mobile or OWA user would receive the infected email, spreading the threat or possibly sending it to other users on the Exchange Server.

Many organizations need to control, secure, and protect ActiveSync and OWA communications for many reasons ranging from basic security hygiene to compliance. For example, ActiveSync and OWA email must be scanned for threats as part of ISO 27001 certification.

The following figure shows that remote users send email and attachments directly to the Exchange Server, bypassing traditional email security.

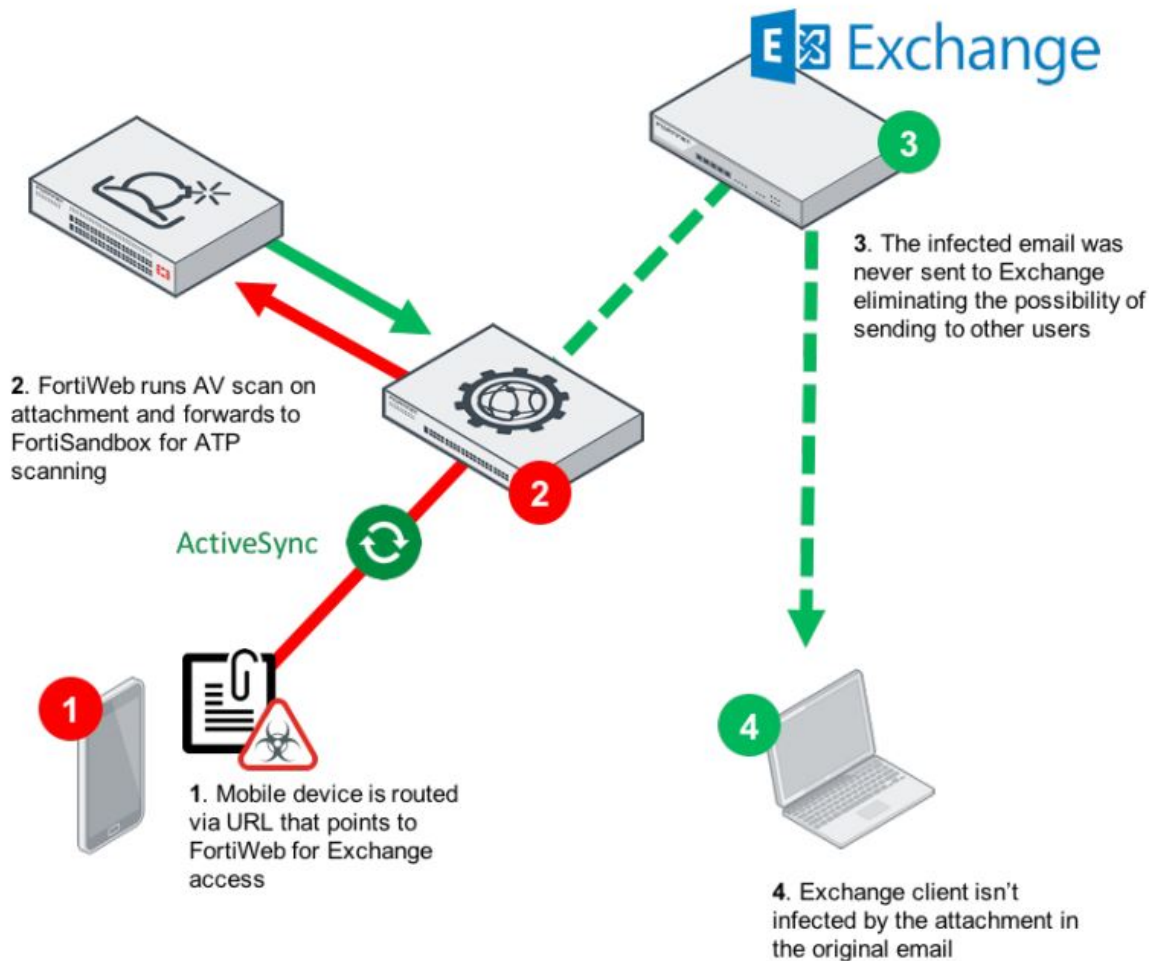


FortiWeb ActiveSync and OWA scanning

In addition to its core web application firewall functionality, FortiWeb can be deployed to publish applications, provide SSO, and manage authentication delegation. Many Fortinet customers use FortiWeb as a replacement for the discontinued Microsoft Threat Management Gateway to publish Microsoft Exchange and other Microsoft applications.

Using this functionality, FortiWeb can be deployed as a proxy for ActiveSync and OWA. This means that any remote mobile user or email client would be directed to FortiWeb. Here FortiWeb would inspect the traffic and intercept any attachments sent from the device or web browser. These attachments are then processed by FortiWeb’s antivirus engine to check for threats. FortiWeb can also be configured to send attachments to Fortinet’s sandboxing solutions for additional scans to detect advanced persistent threats or zero-day attacks.

The following figure shows that FortiWeb is deployed in front of Exchange Server to intercept email traffic from remote devices to scan for threats.



Benefits

By using FortiWeb to protect your ActiveSync-based applications and users accessing email with OWA, you get:

- Proven protection against threats hidden in ActiveSync and OWA attachments
- Mobile Attachment Scanning for Office 365
- Flexible deployment options including VMs, Cloud, and Appliances
- Easy-to-deploy antivirus for Exchange, IBM Notes, and other ActiveSync-based applications
- Integration with FortiSandbox and FortiSandbox Cloud for protection from advanced persistent threats
- Integrated single platform for publishing Microsoft Exchange Server applications and services

Securing OWA with FortiWeb

You can use FortiWeb’s site publishing features to authorize clients that want to connect to web applications such as Microsoft’s Outlook Web App (OWA).

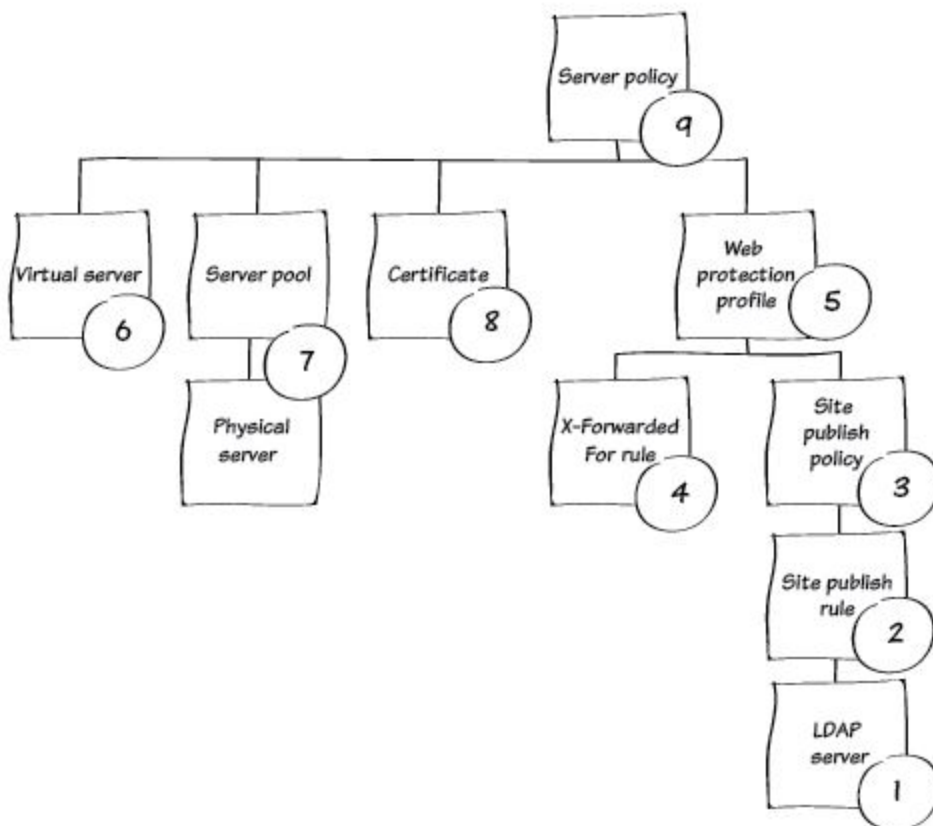
This site publishing feature can replace the web publishing functionality provided by Microsoft’s Threat Management Gateway (TMG). FortiWeb also provides additional security features that protect the application after a successful login.

You create the FortiWeb configuration that publishes and protects web applications using a server policy.

A server policy is made up of several other configuration objects, including:

- Web protection profile — A set of security-related configuration objects.
- Virtual server — The IP address where FortiWeb receives client requests for access to the web application.
- Server pool — A backend server or servers where the web application is located.
- Certificate — Certificate to use for SSL encryption.

The numbers in the illustration correspond to the recipe instructions for the configuration objects.



This guide assumes that:

- Basic configuration is complete, including IP addresses, routing, and DNS information.
- The operating mode is reverse proxy (the destination for requests for the web application is a virtual server IP address on FortiWeb, not the back-end server where the application resides)

FortiWeb configuration

Step 1 - LDAP query

Go to **User > Remote Server > LDAP Server** and create a new entry.

In this example, users log in using their full mail address. Therefore, the Common Name Identifier value is the Active Directory field **userPrincipalName**.

(Other applications or configurations may require different login information.)

To obtain the **Distinguished Name** field:

1. On the domain controller, start the adsiedit.msc tool.
2. Click **Action > Connect to**.
3. Click **OK**.
4. Browse to the **CN=Users** folder.
5. Select a user (for example, CN=Administrator) and then select its properties.
6. Scroll down to **Distinguished Name** field to view the value to use in FortiWeb.

For more information on creating the LDAP query, see [LDAP query best practices and tips](#).

Step 2 - Authentication server pool

Go to **Application Delivery > Site Publish > Authentication Server Pool**.

The screenshot shows the 'New Authentication Server' configuration window. The 'Authentication Validation Method' is set to 'LDAP' and the 'LDAP Server' is 'at-lab-ad'. The 'ID' is set to 'auto'. There are 'OK' and 'Cancel' buttons at the bottom right.

Create a new server pool and add the LDAP server in the pool.

Step 3 - Site publish rule

The screenshot shows the 'Site Publish Rule' configuration window. The 'Name' is 'mail.fortiwlab', 'Published Site Type' is 'Simple String', 'Published Site' is 'mail.fortiwlab', and 'Path' is '/owa'. The 'Client Authentication Method' is 'HTML Form Authentication'. The 'Published Server Log Off Path' is '/owa/logoff.owa'. The 'Authentication Server Pool' is 'dw'. The 'Authentication Delegation' is 'HTTP Basic'. The 'SSO Support' is checked. The 'SSO Domain' is '.fortiwlab'. There are 'OK' and 'Cancel' buttons at the bottom right.

Name is a unique identifier for the rule.

Published Site and **Path** specify the URL the client uses to access OWA. FortiWeb intercepts requests for this URL and forces the clients to pre-authenticate.

Because the path for OWA starts with /owa, the URL is:

`https://mail.fortiwlab/owa`

Published Server Log Off Path specifies the path FortiWeb uses to log off a user. For OWA, it is /owa/logoff.owa.

Please note, for Exchange 2016 CU1 and later, the logoff path is no longer supported by Microsoft. A community-provided workaround is available: <https://social.technet.microsoft.com/Forums/en-US/71462d67-f05b-4d74-af63-b22f3dea35d7/exchange-2016-logoff-does-not-generate-logoff-request>.

Without applying this community-provided workaround, FortiWeb will be unable to identify logoff requests, which means the session cookie will only expire once a user closes their browser and does not use the "Restore previous session" option when opening the browser again.

Client Authentication Method specifies how FortiWeb prompts the client to enter the authentication credentials. For example, via HTTP Basic Authentication or a predefined form (shown at right).

LDAP Server is the LDAP configuration you created earlier.

Authentication Delegation specifies whether FortiWeb sends the credentials the client enters to the back-end server.

For example, select **No Delegation** when the web application has no authentication of its own or uses HTML form-based authentication. Select **HTTP Basic Authentication** to use HTTP Authorization: headers with Base64 encoding to forward the client's credentials to the web application.

Because FortiWeb stores the credentials for the length of the session, it can forward the credentials to other application servers without requiring the client to re-enter the password. To enable this functionality, select SSO Support and specify an SSO Domain value.

Alert Type specifies which login events FortiWeb writes to event log (none, failed only, successful only, or all).

Step 4 - Site publish policy

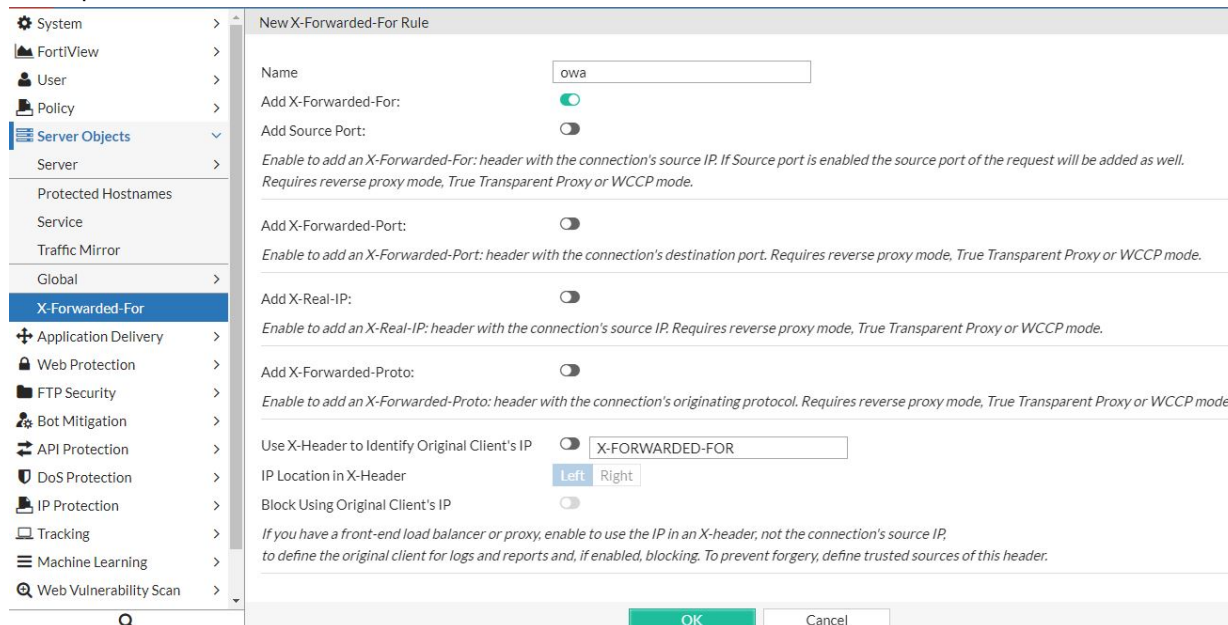
Use a site publish policy to add site publish rules to a web protection profile. The site publish policy allows you to add multiple site publish rules to a policy.

To create a new policy, go to **Application Delivery > Site Publish > Site Publish Policy**. Create a new entry, enter the policy name, and then click OK. Then, you can add one or more site publish rules to the policy.

Step 5 - X-Forwarded-For rule

Because the operating mode is reverse proxy, the source address of all connections from the FortiWeb to the back-end server is the IP address of one of the FortiWeb interfaces.

To provide the client IP address in the log of the back-end server, you can forward the IP address of the client in the request in a `X-Forwarded-For` header.



Go to **Server Objects > X-Forwarded-For > X-Forwarded-For** and create a new entry. Enter a name and select **Add X-Forwarded-For**.

(These settings also provide alternative methods to include this information in requests.)

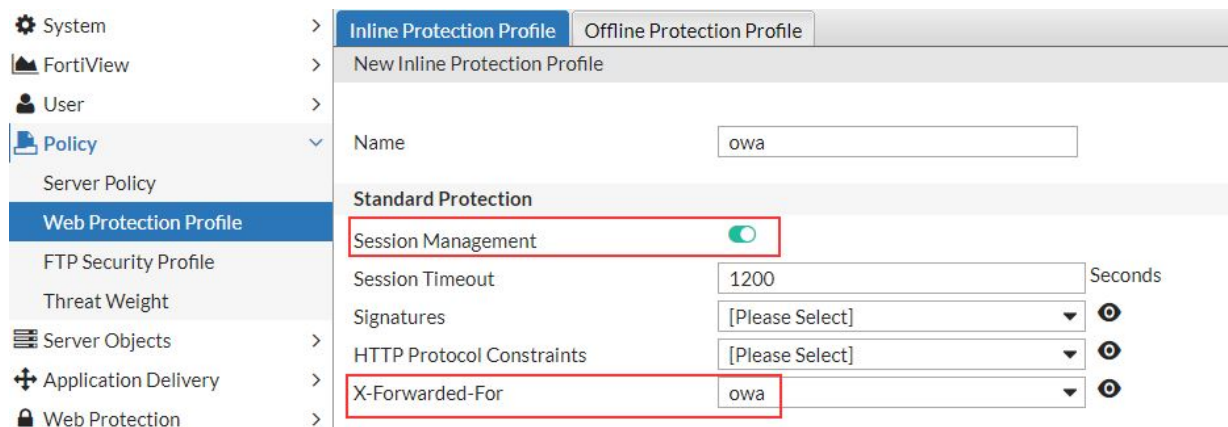
Step 6 - Web protection profile

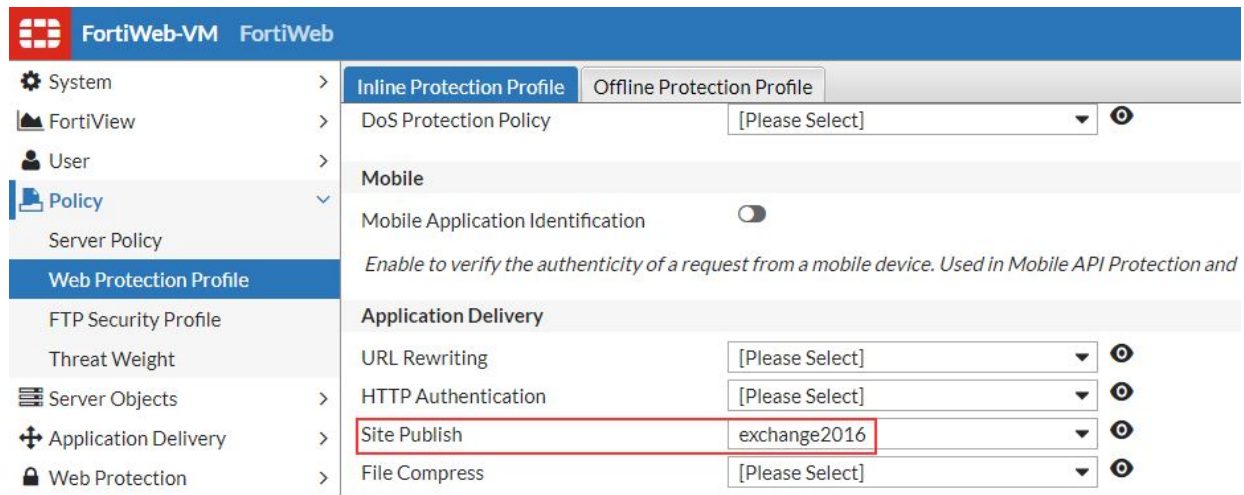
Go to **Policy > Web Protection Profile > Inline Protection Profile**.

Instead of creating a new profile, you can clone the predefined profile for Exchange 2013, and then configure the cloned profile to suit your environment.

Enter a name, enable **Session Management** and select the **X-Forwarded-For** profile you created earlier.

At the bottom of the profile configuration, under **Application Delivery**, for **Site Publish**, select the site publish policy that you created earlier.





Step 7 - Virtual server

Go to **Server Objects > Server > Virtual Server** and create a new entry that specifies the IP address that FortiWeb listens to for connections from the Internet.

Step 8 - Server pool

Go to **Server Objects > Server > Server Pool**. Create a new pool that is a single server pool (the default). Then, add a new pool member by specifying the IP address of the server that runs the published application.

Step 9 - Certificates

To upload certificates or generate certificate signing requests, go to **System > Certificates > Local**.

If you have an official, signed certificate, upload the certificate of the signing authority (CA). Depending on your authority, you also upload the Intermediate CAs.

The FortiWeb Administration Guide includes detailed information about uploading certificates. For example, see “How to offload or inspect HTTPS”.

Step 10 - Server policy

Go to **Policy > Server Policy > Server Policy** and create a new entry.

Select the configuration objects that you created earlier:

- Virtual server
- Server pool
- Certificate
- Web protection profile (inline)

FortiWeb is now listens on the specified IP address and intercepts connections destined for the URL defined in the site publishing rule (in this example, <https://mail.fortiweb.lab/owa>). The client must successfully complete authentication before it can send any further requests to the application server.

You can configure additional security features, but these are outside the scope of this guide.

LDAP query best practices and tips

Edit LDAP Server

Name	<input type="text" value="at-lab-ad"/>
Server IP / Domain	<input type="text" value="192.168.234.21"/>
Server Port	<input type="text" value="3268"/>
Common Name Identifier	<input type="text" value="sAMAccountName"/>
Distinguished Name	<input type="text" value="OU=CONTAINER,DC=DOMAIN,DC=ξ"/>
Bind Type	<input type="text" value="Regular"/>
User DN	<input type="text" value="user@domain.suffix"/>
Password	<input type="password"/>
Filter	<input type="text" value="(&(objectCategory=person)(objectClas"/>
Group Authentication	<input type="checkbox"/>
Secure Connection	<input type="checkbox"/>

In most cases, the AD attribute `sAMAccountName` is the container used for authentication and the appropriate value for **Common Name Identifier**.

However, in some environments, the `userPrincipalName` (email address) is the required or preferred container (for example, for networks that use a domain forest).

For **Server Port**:

- To search for AD objects more efficiently, specify 3268 instead of the default LDAP port 389.
- Fortinet recommends that you transmit user credentials securely by specifying 3269 (for more efficient searching) or the LDAP port 636.

Distinguished Name specifies the Base DN from which to start the LDAP query.

Filter allows you to improve the speed and efficiency of the queries. If **Common Name Identifier** is `userPrincipalName`, use that attribute in the Filter value.

If the query does not work when you specify the LDAP **Distinguished Name** for **User DN**, use the UPN (User Principle Name) instead.

In most cases, the UPN (Email Address) format produces the best results.

Search Filter – `(&(objectCategory=person)(objectClass=user)(sAMAccountName=*))`

For Windows 2003 SP2 and later, the filter can use the string identifier LDAP_MATCHING_RULE_IN_CHAIN (Matching rule OID 1.2.840.113556.1.4.1941). For example:

```
(memberOf:1.2.840.113556.1.4.1941=(CN=Users*))
```

The following example filter matches multiple groups:

```
(&(objectCategory=group)(|(cn=Test*)(cn=Admin*)))
```

The example filters that follow are based on the following example environment:

Directory: DC=domain,DC=com

+ Test_Users

—internet_group

——Matthew Vassallo (user)

—normal_group

——Kenneth Grech (user)

Query multiple groups (method 1)	(& (memberOf=CN=*,OU=Test_Users,DC=domain,DC=com) (sAMAccountName=*))
Query multiple groups (method 2)	(& ((memberOf=CN=normal_group,OU=Test_Users,DC=domain,DC=com) (memberOf=CN=internet_group,OU=Test_Users,DC=domain,DC=com)) (sAMAccountName=%s))
Query all users by sAMAccount type	(sAMAccountType=805306368)
Exclude users in a specific group from the query	(! (memberOf=cn=TestGroup,OU=Groups,DC=DOMAIN,DC=com))
Query for non-disabled users in a group	(& (objectCategory=person) (objectclass=user) (memberOf=CN=All Europe,OU=Global,dc=company,dc=com) (! (userAccountControl:1.2.840.113556.1.4.803:=2)))




Outlook Web App configuration

1. Log in to the Exchange Control Panel. The default URL is: https://<server_name>.<domain_name>.com/ecp
2. Go to **servers > virtual directories**.
3. Select the owa entry, and then click the pencil icon (edit).

servers databases database availability groups **virtual directories** certificates

Select server:

Select type:

NAME	SERVER	TYPE	VERSION	LAST MODIFIED TIME
Autodiscover (Default Web S...	AT-LAB-EXC...	Autodi...	Version 15.0 (Build 516...	6/10/2014 4:57 PM
ecp (Default Web Site)	AT-LAB-EXC...	ECP	Version 15.0 (Build 516.32)	6/11/2014 5:40 PM
EWS (Default Web Site)	AT-LAB-EXC...	EWS	Version 15.0 (Build 516.32)	6/10/2014 4:57 PM
Microsoft-Server-ActiveSync (...)	AT-LAB-EXC...	EAS	Version 15.0 (Build 516.32)	6/10/2014 4:57 PM
OAB (Default Web Site)	AT-LAB-EXC...	OAB	Version 15.0 (Build 516.32)	6/10/2014 4:57 PM
owa (Default Web Site)	AT-LAB-EXC...	OWA	Version 15.0 (Build 516.32)	6/11/2014 5:39 PM
PowerShell (Default Web Site)	AT-LAB-EXC...	Power...	Version 15.0 (Build 516.32)	6/10/2014 4:58 PM

Autodiscover (Default Web Site)
Authentication: Basic, NTLM, Integrated Windows, Windows SharePoint Security, OAuth

4. Select authentication, and then select Use one or more standard authentication methods and Basic authentication.

Use one or more standard authentication methods

- Integrated Windows authentication
- Digest authentication for Windows domain servers
- Basic authentication

Use forms-based authentication

Logon format:

- Domain\user name
- User principal name (UPN)
- User name only

Logon Domain

5. Select Save.

Outlook Web Access administration prompts to make the same change to the /ecp virtual folder.

Select the ecp entry and make the same setting changes as you did for the owa entry.

Securing ActiveSync with FortiWeb

As part of its core publishing functionality FortiWeb allows publishing ActiveSync as well. This means any access to the application over ActiveSync is proxied through FortiWeb which secures the connection, enforcing multiple security rules including scanning email attachments with Antivirus and FortiSandbox. FortiWeb can also be used for its publishing functionality for SSO and authentication delegation.

This guide configuration discusses two use cases – when the requirement is specifically for ActiveSync antivirus and sandboxing scanning or when SSO and authentication delegation is also required.

Use Case 1: Scanning ActiveSync Email Attachments

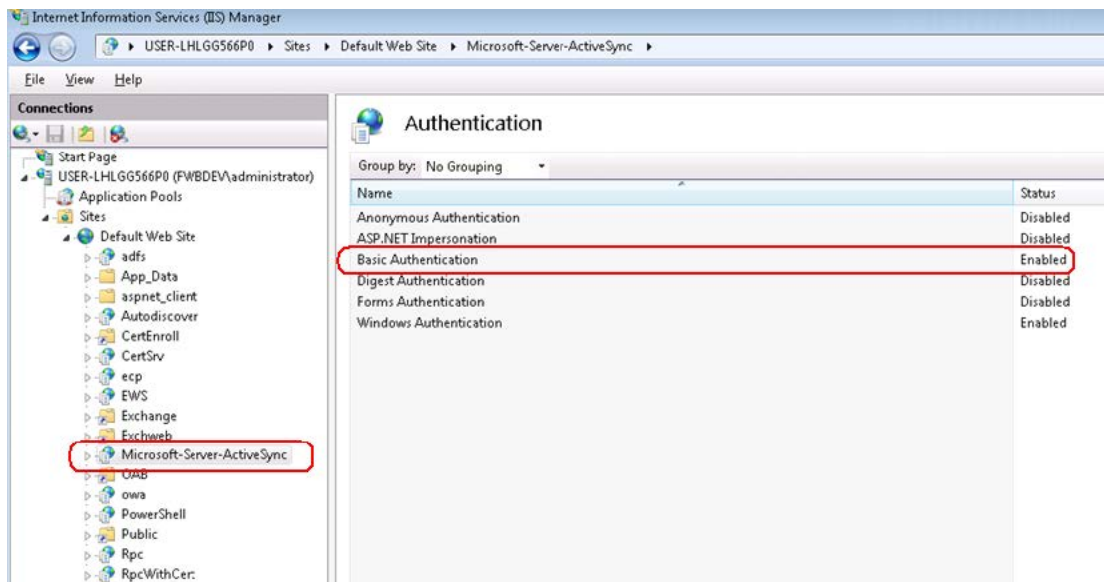
As ActiveSync delivers emails to devices, organizations need to make sure email attachments are scanned to ensure they do not carry any malware.

FortiWeb provides the ability to extract attachments from the mobile to mail server sessions, scan them using its embedded Antivirus engine, and send them to FortiSandbox for additional scanning.

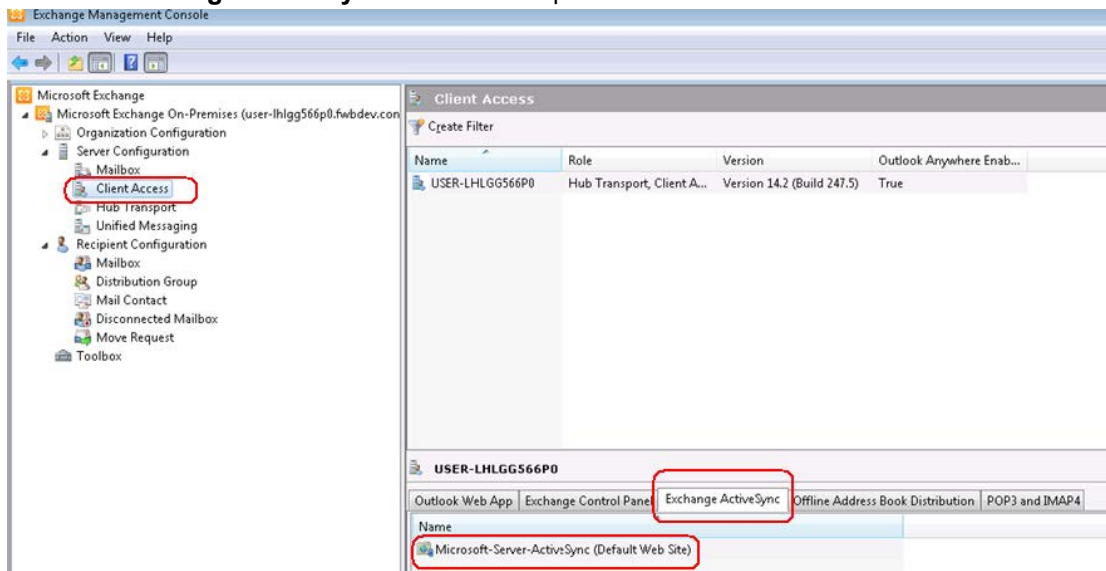
First, make sure your web server supports ActiveSync and configured correctly. Here is an example for Microsoft Exchange:

Exchange 2010

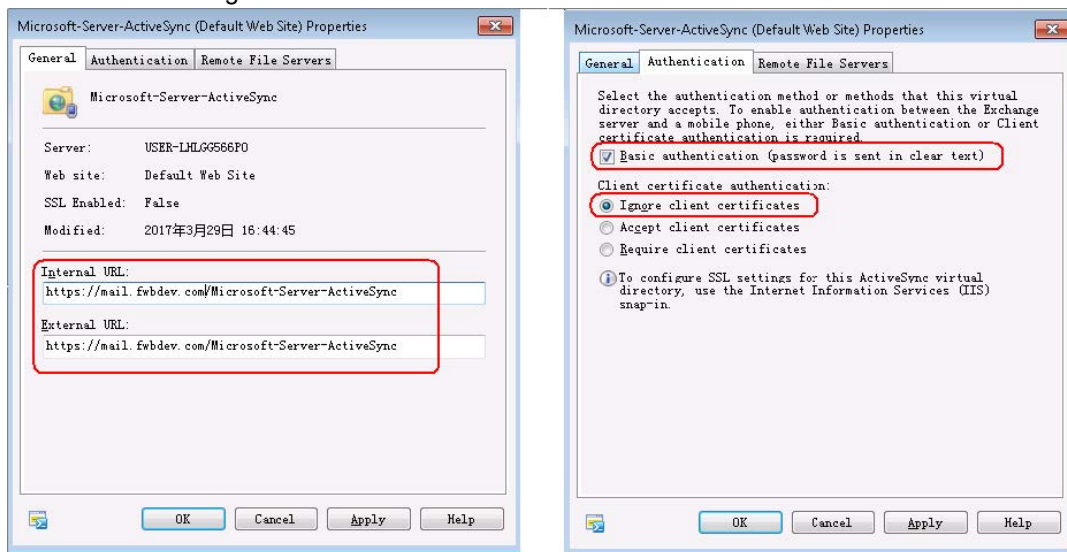
1. Open IIS Manager.
 - a. Go to **Microsoft-Server-ActiveSync**.
 - b. Make sure **Basic Authentication** is enabled.



2. Open Exchange Management Console.
 - a. Go to **Client Access**.
 - b. Switch to **Exchange ActiveSync** on the bottom panel.



- c. Double click **Microsoft-Server-ActiveSync (Default Web Site)**.
- d. Make sure:
 - i. URLs are configured correctly.
 - ii. Basic authentication is enabled.
 - iii. Client certificate is ignored.

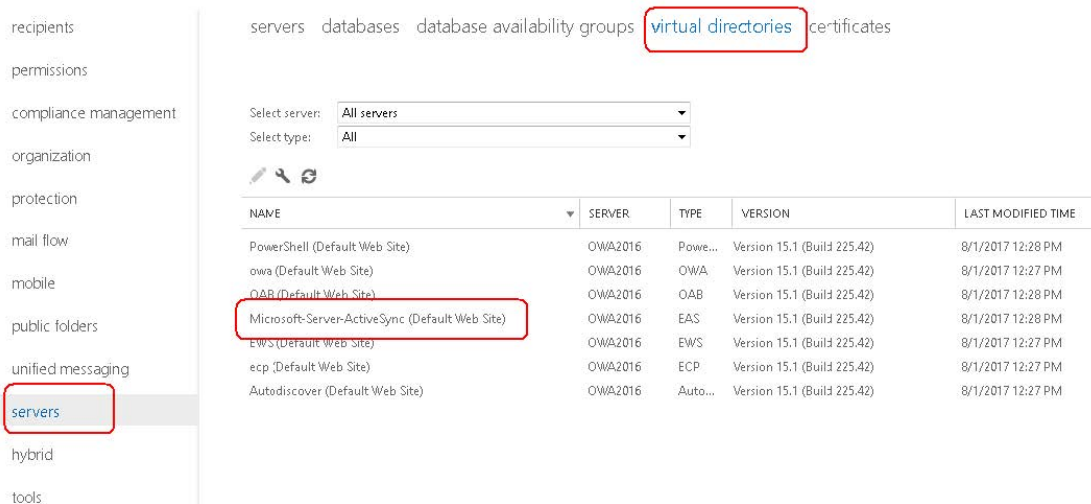


Exchange 2013/2016/2019

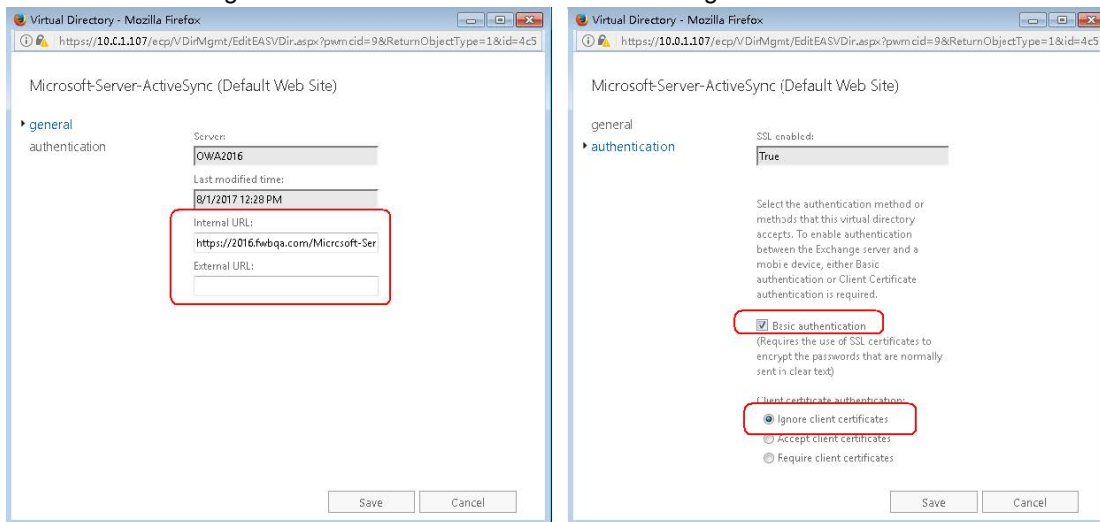
1. Open your browser, and access Exchange admin center <https://<exchange.server.com>/ecp>.
2. Log in with administrator credentials.

3. Go to Microsoft-Server-ActiveSync (Default Web Site).

Exchange admin center



4. Make sure the configurations are the similar to those of Exchange 2010 above.



FortiWeb Configuration

First, configure the File Security policy.

1. Enable **Trojan Detection** for additional security. Make sure you enable Antivirus Scan and FortiSandbox.
2. Enable **Scan attachments in Email** and choose **ActiveSync** in Protocol (possibly OWA too if you're using FortiWeb to publish Exchange OWA as well).

System	File Security Policy	File Security Rule
FortiView	Edit File Security Policy	
User	Name	xxfile
Policy	Action	Alert & Deny
Server Objects	Block Period	60 (1~3600)(Seconds)
Application Delivery	Severity	Low
Web Protection	Trigger Action	Please Select
Known Attacks	Trojan Detection	<input checked="" type="checkbox"/>
Advanced Protection	Antivirus Scan	<input checked="" type="checkbox"/>
Cookie Security	Send Files to FortiSandbox	<input checked="" type="checkbox"/>
Input Validation	Send Files to ICAP Server	<input type="checkbox"/>
Parameter Validation	Hold Session While Scanning File	<input type="checkbox"/>
Hidden Fields	Scan Attachments in Email	<input checked="" type="checkbox"/>
File Security	Protocol	OWA <input type="checkbox"/> ActiveSync <input checked="" type="checkbox"/> MAPI <input type="checkbox"/>
Protocol		

Now, attach the File Security policy to the Web Protection Profile. For more information on File Security, see **Limiting file uploads** in [FortiWeb Administration Guide](#).

Next, create a new server policy. ActiveSync is usually used with SSL. So the front end and backend should be configured with HTTPS.

1. Configure the front end (towards the client) options.

System	>	Edit Policy
FortiView	>	
User	>	
Policy	>	Network Configuration
Server Policy	>	Policy Name: <input type="text" value="dwg_policy"/>
Web Protection Profile	>	Deployment Mode: <input type="text" value="Single Server/Server Pool"/>
FTP Security Profile	>	Virtual Server: <input type="text" value="vserver"/>
Threat Weight	>	Server Pool: <input type="text" value="Win2008_30.13"/>
Server Objects	>	Protected Hostnames: <input type="text" value="[Please Select...]"/>
Application Delivery	>	Client Real IP: <input type="checkbox"/>
Web Protection	>	<i>Enable to use the client source IP and port when Configure FortiWeb as the default gateway on t</i>
FTP Security	>	Syn Cookie: <input checked="" type="checkbox"/>
Bot Mitigation	>	Half Open Threshold: <input type="text" value="200"/>
API Protection	>	HTTP Service: <input type="text" value="HTTP"/>
DoS Protection	>	HTTPS Service: <input type="text" value="HTTPS"/>
IP Protection	>	HTTP/2: <input type="checkbox"/>
Tracking	>	Enable Multi-certificate: <input type="checkbox"/>
Machine Learning	>	Certificate: <input type="text" value="Fortinet_Factory"/>
Web Vulnerability Scan	>	Certificate Intermediate Group: <input type="text" value="[Please Select...]"/>
Log&Report	>	
Monitor	>	

2. Configure the backend (towards the server pool) options.

Edit Server Pool Rule

ID	1	
Status	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Maintenance"/>	
Server Type	<input checked="" type="button" value="IP"/> <input type="button" value="Domain"/>	
IP	<input type="text" value="10.101.30.13"/>	
Port	<input type="text" value="443"/>	
Connection Limit	<input type="text" value="0"/>	(Concurrent Connections)(0 - 1048576)
<i>Maximum number of concurrent connections to the backend server. Input 0 for no con</i>		
Weight	<input type="text" value="1"/>	(1~9999)
<i>Assigns relative preference among members—higher values are more preferred and ar</i>		
Inherit Health Check	<input checked="" type="checkbox"/>	
Health Check Domain Name	<input type="text"/>	
Backup Server	<input type="checkbox"/>	
<i>Set to Enable to designate this server as a last server to be used when all other servers</i>		
Proxy Protocol	<input type="checkbox"/>	
HTTP/2	<input type="checkbox"/>	
SSL	<input checked="" type="checkbox"/>	
<i>Enable to use SSL/TLS for connections between FortiWeb and the pool member</i>		
Client Certificate	<input type="text" value="[Please Select]"/>	
<i>Required only if a valid client certificate is required to connect to this pool member.</i>		
Advanced SSL settings		
Show advanced settings		

Now, open the mail application on your phone and test.

Use Case 2: Managing Authentication and SSO to ActiveSync

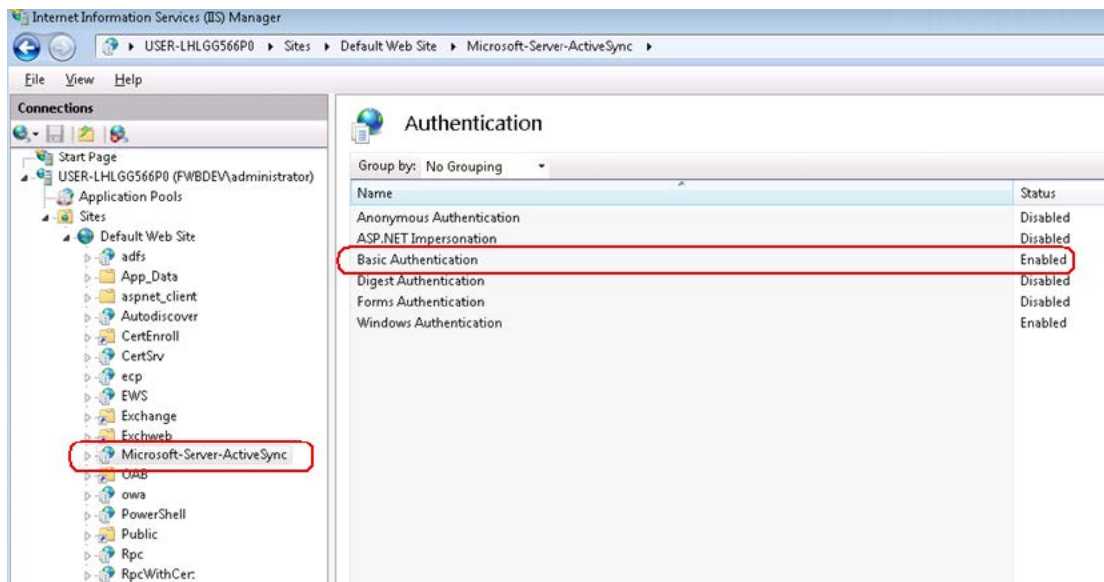
Many organizations tightly control how Microsoft applications are used by publishing the application through TMG, Microsoft’s Threat Management Gateway that allows secure access to these applications. With TMG EOL’d and sunsetting customers can use FortiWeb as a replacement.

Customers that want to control the authentication and SSO for ActiveSync, usually as part of publishing other components of the Exchange server should use FortiWeb’s Site Publish feature.

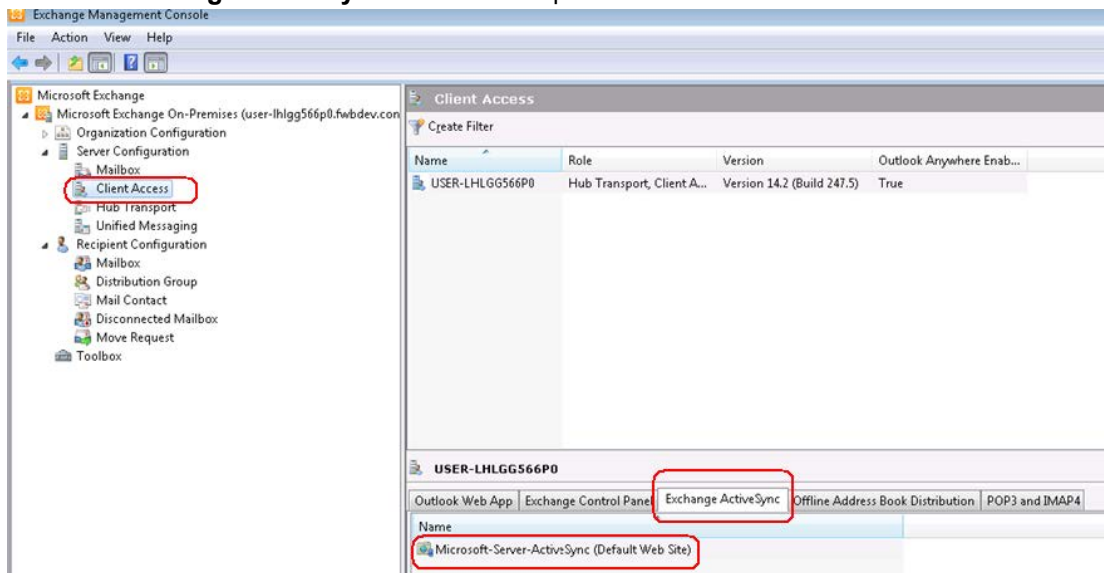
First, make sure your Microsoft Exchange is configured correctly:

Exchange 2010

1. Open IIS Manager.
 - a. Go to **Microsoft-Server-ActiveSync**.
 - b. Make sure **Basic Authentication** is enabled.

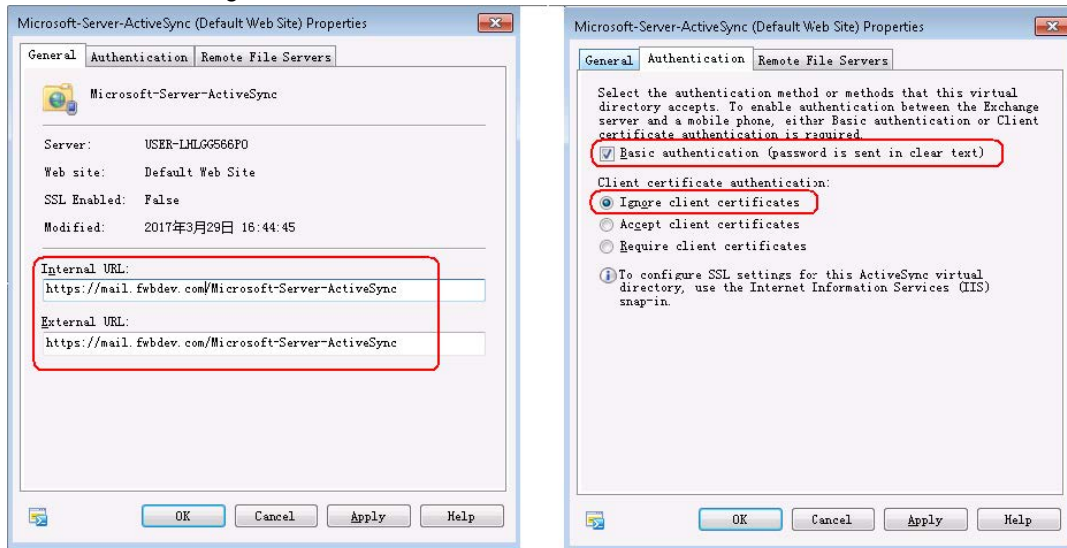


2. Open Exchange Management Console.
 - a. Go to **Client Access**.
 - b. Switch to **Exchange ActiveSync** on the bottom panel.



- c. Double click **Microsoft-Server-ActiveSync (Default Web Site)**.
- d. Make sure:
 - i. URLs are configured correctly.
 - ii. Basic authentication is enabled.

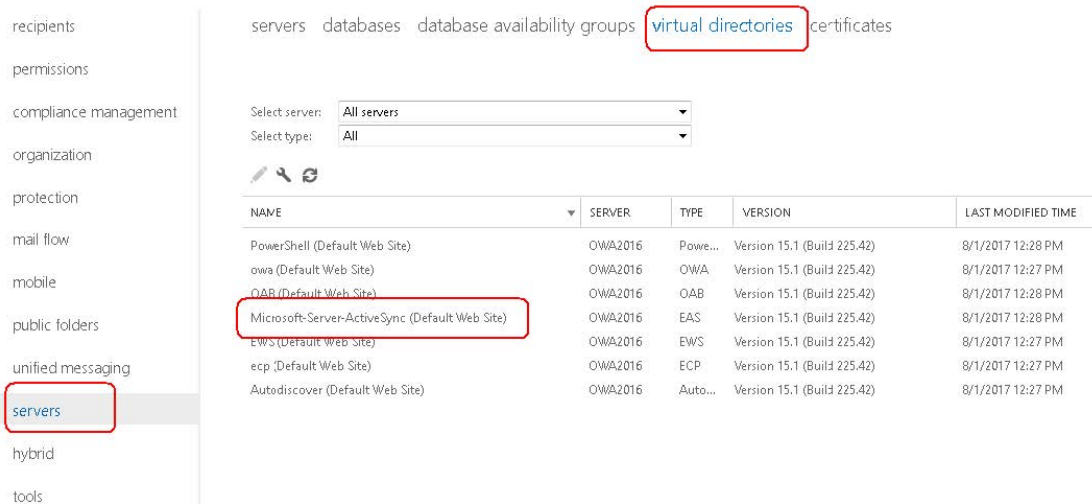
iii. Client certificate is ignored.



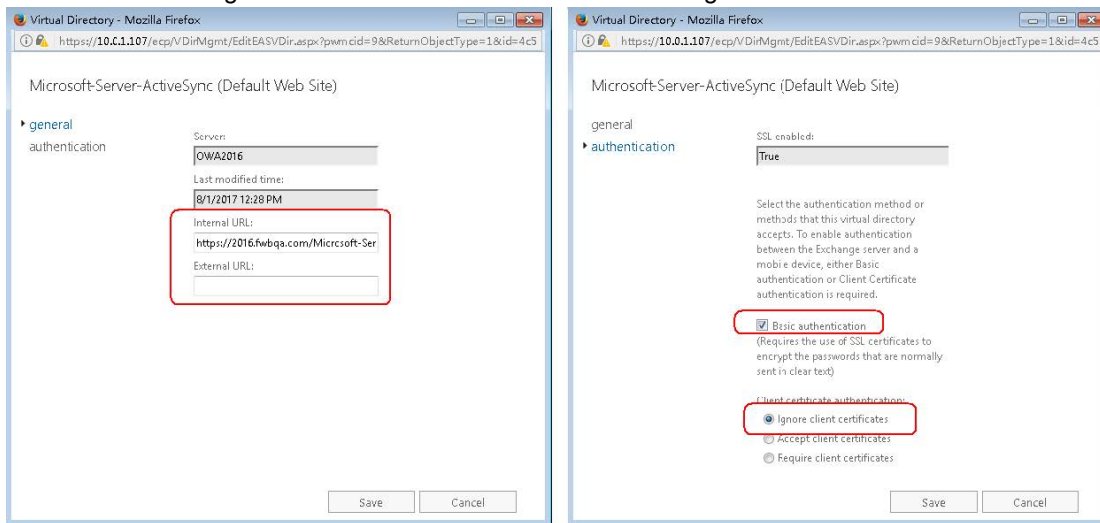
Exchange 2013/2016/2019

1. Open your browser, and access Exchange admin center <https://<exchange.server.com>/ecp>.
2. Log in with administrator credentials.
3. Go to **Microsoft-Server-ActiveSync (Default Web Site)**.

Exchange admin center



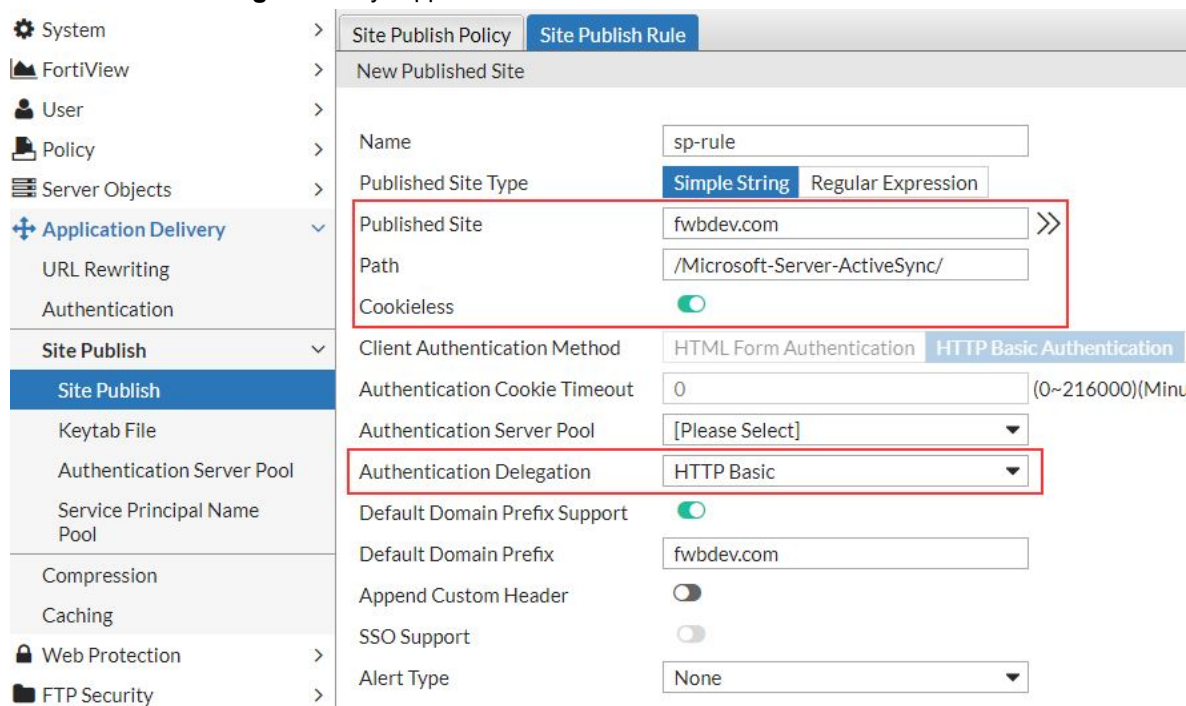
4. Make sure the configurations are the similar to those of Exchange 2010 above.



FortiWeb Configuration

First, configure a Site Publish policy:

- **Published Site** should be the domain name of the URL above.
- **Path** should be consistent with the URL above.
- **Cookieless** should be enabled so that clients can access to Microsoft Exchange servers through Exchange ActiveSync.
- **Authentication Delegation** only supports HTTP Basic.



Now, attach the Site Publish policy to the Web Protection Profile.

Next, create a new server policy. ActiveSync is usually used with SSL, so the front end and backend should be configured with HTTPS.

1. Configure the front end (towards the client) options.

The screenshot shows the FortiWeb configuration interface for editing a policy. The left sidebar contains a navigation menu with the following items: System, FortiView, User, Policy (expanded), Server Policy (selected), Web Protection Profile, FTP Security Profile, Threat Weight, Server Objects, Application Delivery, Web Protection, FTP Security, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Machine Learning, Web Vulnerability Scan, Log&Report, and Monitor. The main content area is titled 'Edit Policy' and shows the 'Network Configuration' section. The settings are as follows:

Setting	Value
Policy Name	dwg_policy
Deployment Mode	Single Server/Server Pool
Virtual Server	vserver
Server Pool	Win2008_30.13
Protected Hostnames	[Please Select...]
Client Real IP	<input type="checkbox"/>
<i>Enable to use the client source IP and port when Configure FortiWeb as the default gateway on t</i>	
Syn Cookie	<input checked="" type="checkbox"/>
Half Open Threshold	200
HTTP Service	HTTP
HTTPS Service	HTTPS
HTTP/2	<input type="checkbox"/>
Enable Multi-certificate	<input type="checkbox"/>
Certificate	Fortinet_Factory
Certificate Intermediate Group	[Please Select...]

2. Configure the backend (towards the server pool) options.

Edit Server Pool Rule

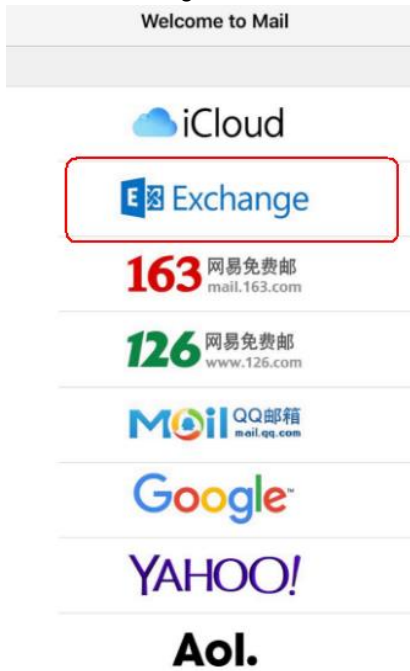
ID	1
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Maintenance
Server Type	<input checked="" type="radio"/> IP <input type="radio"/> Domain
IP	<input type="text" value="10.101.30.13"/>
Port	<input type="text" value="443"/>
Connection Limit	<input type="text" value="0"/> (Concurrent Connections)(0 - 1048576) <i>Maximum number of concurrent connections to the backend server. Input 0 for no con</i>
Weight	<input type="text" value="1"/> (1~9999) <i>Assigns relative preference among members—higher values are more preferred and ar</i>
Inherit Health Check	<input checked="" type="checkbox"/>
Health Check Domain Name	<input type="text"/>
Backup Server	<input type="checkbox"/> <i>Set to Enable to designate this server as a last server to be used when all other servers</i>
Proxy Protocol	<input type="checkbox"/>
HTTP/2	<input type="checkbox"/>
SSL	<input checked="" type="checkbox"/> <i>Enable to use SSL/TLS for connections between FortiWeb and the pool member</i>
Client Certificate	<input type="text" value="[Please Select]"/> <i>Required only if a valid client certificate is required to connect to this pool member.</i>

[Advanced SSL settings](#)

[Show advanced settings](#)

Now, open the mail application on your phone and test. The following uses iPhone as an example

1. Open the Mail app.
2. Choose Exchange.



3. Input your credentials.

Verifying

Email she@fwbdev.com

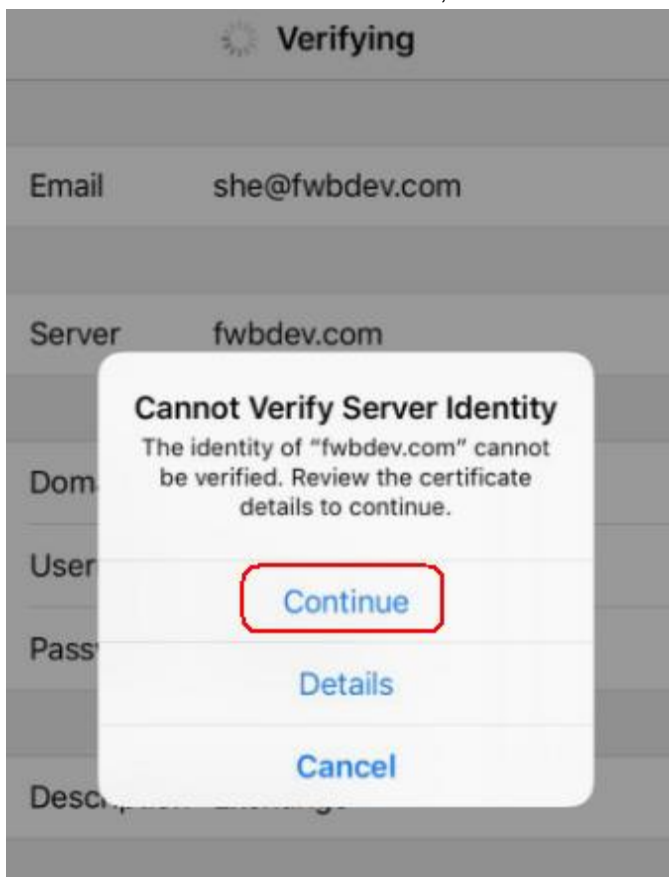
Password ●●●●●●●

Description Exchange

- Sometimes, a re-check form would pop up. Input your info again.

A screenshot of a mobile login form. The form consists of several input fields stacked vertically. The first field is labeled 'Email' and contains the text 'she@fwbdev.com'. The second field is labeled 'Server' and contains 'fwbdev.com'. The third field is labeled 'Domain' and contains the text 'Optional'. The fourth field is labeled 'Username' and contains 'she'. The fifth field is labeled 'Password' and contains a series of black dots. The form is presented on a light gray background.

- If the FortiWeb certificate is not trusted, there will be a warning page. Press **Continue**.



- Access now is secured by FortiWeb.



FORTINET®



Copyright© 2020 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.