

## How to publish Exchange 2013 with Sophos UTM

- Go to the Web Admin Console of your Sophos UTM
  - Login
  - Go to “Webserver Protection”
  - Click on “Reverse Authentication”
    - Create new authentication profile

**Edit Authentication Profile**

Name: my-reverse-authentication

**Virtual Webserver**

Mode: Form

Form Template: Default Template

**Users / Groups**

Active Directory Users

DND	DND	DND
DND	DND	DND
DND	DND	DND
DND	DND	DND

**Real Webserver**

Mode: Basic

User name affix: Suffix

Suffix: @my-domain.com

**User Session**

Session Timeout: ☒ Limit to: 10 Minutes

Session Lifetime: ☒ Limit to: 8 Hours

Comment:

Save Cancel

- Click on “Web Application Firewall”
  - Click on tab “Real Webserver”
- Create your real webserver by entering your exchange 2013 server

**Edit Real Webserver**

Name: mail

Host: Exchange 2013

Type: Encrypted (HTTPS)

Port: 443


Comment:

Advanced

Save Cancel

- Create the appropriate site path routing
  - Click on tab “Site Path Routing”
  - Create the following 8 paths:

### **/microsoft-server-activesync**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /microsoft-server-activesync  
*Real Webservers:*  Exchange2013  
  
*Access control:* off

### **/autodiscover**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /autodiscover  
*Real Webservers:*  Exchange2013  
  
*Access control:* off

### **/ecp**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /ecp  
*Real Webservers:*  Exchange2013  
  
*Reverse Authentication Profile:* my-reverse-authentication  
*Access control:* off


### **/ews**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /ews  
*Real Webservers:*  Exchange2013  
  
*Access control:* off

### **/oab**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /oab  
*Real Webservers:*  Exchange2013  
  
*Access control:* off

### **/owa**


*Virtual Webserver:* mail.my-domain.com  
*Path:* /owa  
*Real Webservers:*  Exchange2013  
  
*Reverse Authentication Profile:* my-reverse-authentication  
*Access control:* off

## **/rpc**

*Virtual Webserver:* mail.my-domain.com  
*Path:* /rpc  
*Real Webservers:*  Exchange2013  
*Access control:* off

## **/ (Exchange2013)**

This is a default Site Path Route. It is used if no other Site Path Route matches requests for this Virtual Webserver.

*Virtual Webserver:* mail.my-domain.com  
*Path:* /  
*Real Webservers:*  Exchange2013  
*Access control:* off

- Create the virtual webservers
  - Click on tab "Virtual Webservers"

**Edit Virtual Webserver**

Name: mail.my-domain.com

Interface: Red (Address)

Type: Encrypted (HTTPS) & Redirect

Port: 443

Certificate: mail.my-domain.com

**Domains**

- mail.my-domain.com

**Real Webservers**

- ☒ Exchange2013 **enabled**

Firewall Profile: Advanced Outlook Protection

Comment:

**Advanced**

- ☐ Disable Compression Support
- ☒ Rewrite HTML
- ☒ Rewrite cookies
- ☒ Pass Host Header

☒ Save ☐ Cancel

- Create new firewall profile
  - Click on tab "Firewall Profiles"
  - Create a firewall profile similar to the following one edit the virtual webserver accordingly

The screenshot shows the 'Edit Firewall Profile' window for a profile named 'Advanced Outlook Protection'. The window contains several configuration options:

- Name:** Advanced Outlook Protection
- ☒ **Pass Outlook Anywhere**
- Mode:** Reject
- ☒ **Common Threats Filter**
- ☐ **Rigid Filtering**
- Skip Filter rules** (with a list icon and a plus sign)
- ☐ **Cookie Signing**
- ☐ **Static URL Hardening**
- ☐ **Form Hardening**
- ☒ **Antivirus**
  - Mode:** Single Scan
  - Direction:** Downloads only
- ☐ **Block unscannable content**
- ☒ **Limit scan size**
  - Megabytes:** 25
- ☐ **Block clients with bad reputation**
- Comment:** (empty text box)
- Threat Filter Categories** (expanded section):
  - ☐ Protocol Violations
  - ☐ Protocol Anomalies
  - ☒ Request Limits
  - ☐ HTTP Policy
  - ☒ Bad Robots
  - ☒ Generic Attacks
  - ☒ SQL Injection Attacks
  - ☒ XSS Attacks
  - ☒ Tight Security
  - ☒ Trojans
  - ☐ Outbound

At the bottom right, there are 'Save' and 'Cancel' buttons.

- Change the authentication method on your Exchange2013 server

The following will change the authentication method to forms with UTM and provide single sign on for internal users

- Start Exchange Administration PowerShell on the Exchange server
- Enter the following commands. One at a time.

```
Get-EcpVirtualDirectory | Set-EcpVirtualDirectory -AdfsAuthentication $false -
BasicAuthentication $true -DigestAuthentication $false -FormsAuthentication
$false -WindowsAuthentication $true
```

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -AdfsAuthentication $false -  
BasicAuthentication $true -DigestAuthentication $false -FormsAuthentication  
$false -WindowsAuthentication $true
```

- Run: iisreset /noforce

Try it.

- Next step can be: ADFS and Claims based authentication with ADFS and WebApplicationProxy (Server Role in Windows2012 R2)

[https://technet.microsoft.com/en-us/library/dn635116\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn635116(v=exchg.150).aspx)