

► *Handbook*

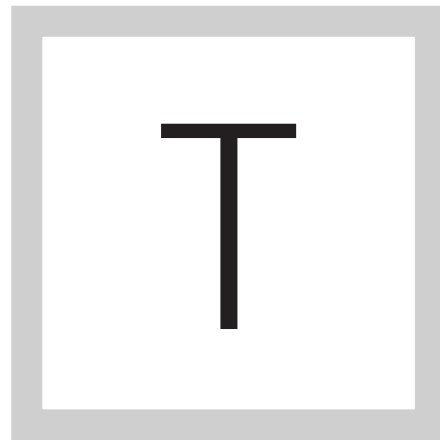
SHORE UP YOUR OFFICE 365 ATTACK SURFACE

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder



THE MICROSOFT OFFICE 365 security features are robust, but may not offer the granularity some enterprises need. In this eGuide, experts review Microsoft's cloud-based productivity suite, a step-by-step process to configure Office 365 authentication with PowerShell, and Client Access policies. Read on to learn how to mediate common email security issues and what implementing Microsoft Office 365 can do for your business.

AN INTRODUCTION TO MICROSOFT OFFICE 365 SECURITY

Dave Shackelford

With the end of Windows XP, more organizations are migrating to new operating systems, and in turn taking the opportunity to explore different service models for applications. While there are numerous cloud-based office applications available today, one that is getting a lot of traction and attention is Microsoft Office 365.

This tip explores the key Microsoft Office 365 security technologies, as well as the potential security issues enterprises should be aware of and how to overcome them.

OFFICE 365 SECURITY: FEATURES

Microsoft Office 365 runs in a typical multi-tenant public cloud environment. Active Directory containers are used for isolation and segregation of customer data, but Microsoft also makes a separate Office 365 environment available to customers at additional cost.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

[Home](#)[An introduction to Microsoft Office 365 security](#)[Configure Office 365 authentication with PowerShell](#)[Secure Office 365 with the Client Access Policy Builder](#)

All access to the Office 365 infrastructure is performed via strict role-based access control (RBAC) techniques that use a “lockbox” approach. This is where engineers request access for specific tasks that are independently verified and vetted each time, with access duration and monitoring applied.

All network connections to Office 365 also use SSL/TLS over the Internet by default. Within the Office 365 environment, stored data is encrypted with BitLocker, Microsoft’s encryption feature that leverages the Advanced Encryption Standard algorithm.

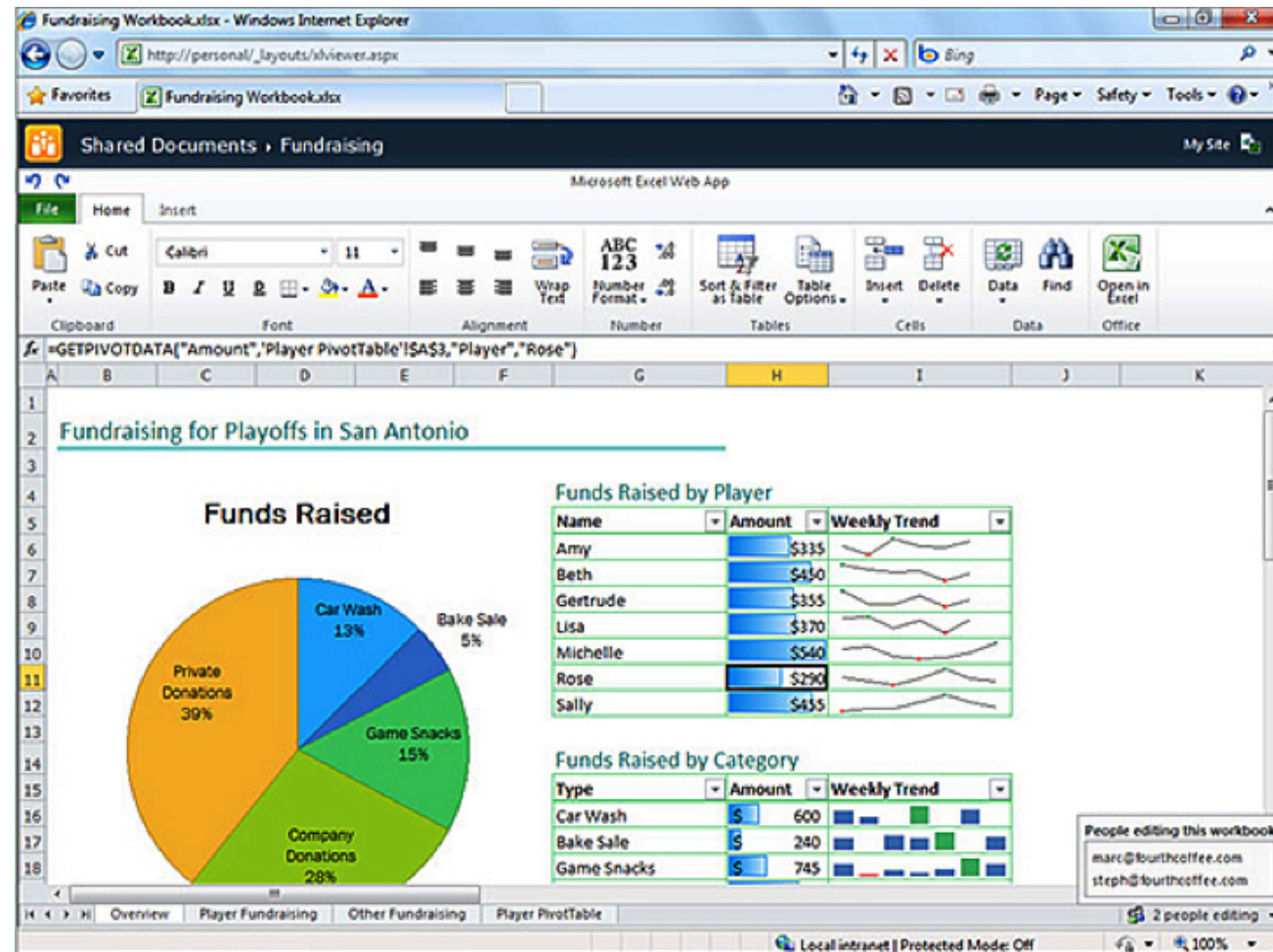
Office 365 has customizable encryption policies that can be applied to stored content or used to sign documents. The Windows Rights Management Service allows administrators to specify who can access encrypted content, what type of access a user has and when they can access the content. In addition, Microsoft now offers configurable encryption for email. Office 365 Message Encryption is built on Azure Rights Management, which allows administrators to flexibly control when and how encryption is applied depending on a number of customizable attributes, including content keywords or internal vs. external recipients.

Home

An introduction to Microsoft Office 365 security

Configure Office 365 authentication with PowerShell

Secure Office 365 with the Client Access Policy Builder



Spreadsheet editing using the Office 365 Excel Web App

[Home](#)[An introduction to Microsoft Office 365 security](#)[Configure Office 365 authentication with PowerShell](#)[Secure Office 365 with the Client Access Policy Builder](#)

Administrators can control all access to Office 365 by taking advantage of the built-in Active Directory identity platform from Azure, or by integrating with internal Active Directory stores using on-premises Active Directory. Other directory stores and identity systems include Active Directory Federation Services and third-party Secure Token Services, like those from vendors SecureAuth or Swivel. More advanced federation can be configured to support true single sign-on, allowing enterprise users to authenticate to Office 365 with their existing domain credentials while also tying in multifactor authentication options and client-based access controls for simple NAC functionality. For example, users trying to access Office 365 from public wireless connections or public computers could be restricted using client access policies.

OFFICE 365 SECURITY: BENEFITS

One of the more compelling features within Office 365 is data loss prevention (DLP) policy control. With Exchange Online and Outlook 2012, security administrators can develop DLP rules that alert users when they are trying to send email with content or attachments matching well-known or custom patterns for sensitive information. Content can be allowed with a warning, allowed with an explicit policy override that notifies administrators, or blocked

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

entirely based on sender, receiver, internal and external addresses, domains and more. DLP is currently being developed for Microsoft OneDrive, a cloud-based storage drive accessed from users' mobile devices, laptops and desktops. The OneDrive DLP features are expected to debut this month.

Office 365 also has a powerful set of e-discovery policies, available within the Office 365 eDiscovery Center. Access to the eDiscovery Center can be delegated to a compliance or legal officer using RBAC, and the tools allow for simple searches across all Office 365 data storage including email, documents and site mailboxes, with the ability to preserve data. Antispam and antimalware controls are also built into Office 365, and administrators can configure some aspects, such as blocking sensitivity and alerting.

OFFICE 365 SECURITY: DRAWBACKS

One downside to the service is the lack of malware and spam email evidence available to customers from Microsoft. As Microsoft blocks attachments and spam emails, it does not provide the blocked content to customers for threat intelligence and malware analysis. For larger organizations seeking to bolster security intelligence by mining spam and phishing data, this may prove to be a big downside to an otherwise valuable security offering.

[Home](#)[An introduction to Microsoft Office 365 security](#)[Configure Office 365 authentication with PowerShell](#)[Secure Office 365 with the Client Access Policy Builder](#)

The DLP service, while admin-friendly, is fairly simplistic, which may prove to be less granular and configurable than some organizations need.

Finally, while Microsoft has met a number of compliance requirements ranging from EU data protection laws to HIPAA and ISO 27001, there is still some risk in placing sensitive data into a cloud environment, and organizations will continue to be liable for their regulatory concerns regardless of the outsourcing model chosen.

CONCLUSION

Overall, Office 365 aims to offer a powerful and flexible set of cloud application services that include a broad range of security features. As more security features are added, with additional configuration capabilities for consumers, organizations that transition to Office 365 in the coming years will find that its security is more than capable of meeting most enterprises' needs.

DAVE SHACKLEFORD is the owner and principal consultant of Voodoo Security LLC; lead faculty at IANS; and a SANS analyst, senior instructor and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering, and is a VMware vExpert with extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO at Configuresoft, as CTO at the Center for Internet Security, and as a security architect, analyst and manager for several Fortune 500 companies. Dave is

[Home](#)[An introduction to Microsoft Office 365 security](#)[Configure Office 365 authentication with PowerShell](#)[Secure Office 365 with the Client Access Policy Builder](#)

the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, as well as the co-author of *Hands-On Information Security* from Course Technology. Recently, he co-authored the first published course on virtualization security for the SANS Institute. He currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

CONFIGURE OFFICE 365 AUTHENTICATION WITH POWERSHELL

Michel De Rooij

Multifactor Authentication is a must-have for services based in the cloud, especially for accounts with administrative purposes. We have already covered what Office 365 Multifactor Authentication is and how to configure it in Office 365 tenants with the Office 365 admin center, and we briefly showed the end user experience. Now we will look at how we can use the Azure Active Directory Module for Windows PowerShell to configure Office 365 authentication with MFA.

Azure Active Directory Module for Windows PowerShell (AADMPS)

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

enables organizations to not only configure MFA for existing end users who use PowerShell, but also enhance their current provisioning process with MFA options. By pre-configuring MFA, administrators can prevent end users from having to go through the initial MFA setup process and use their currently configured mobile phone or office number for verification.

You'll need to download and install AADMPS before you can start using it and its PowerShell cmdlets. The module is available for x64, but there is also an x86 version.

After installation, you will have an extra shortcut called Windows Azure Active Directory Module for Windows PowerShell. This will start a PowerShell session with the module loaded. You could also import the module in an existing PowerShell session using Import-Module MSOnline.

The next step will be to connect to your Office 365 tenant using Connect-MsolService, providing valid administrator credentials.

CONFIGURE OFFICE 365 MULTIFACTOR AUTHENTICATION

To configure the Office 365 authentication for MFA, you need to define a strong authentication object:

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

```
$st= New-Object Microsoft.Online.Administration.  
StrongAuthenticationRequirement
```

```
$st.RelyingParty= '*'
```

After that, enabling MFA for an end user with the User Principal Name michel@test.com is as simple as:

```
Set-MSolUser -UserPrincipalName michel@test.com -StrongAuthenti-  
cationRequirements @($st)
```

To disable MFA, use this cmdlet:

```
Set-MSolUser -UserPrincipalName michel@test.com  
-StrongAuthenticationRequirements @()
```

This will only enable Office 365 Multifactor Authentication for those end users, and they need to go through the MFA setup process when logging in. Administrators can also preconfigure MFA for specific contact methods. In those cases,

we need to enhance the previous cmdlets as follows:

```
$st= New-Object  
Microsoft.Online.Administration.StrongAuthenticationRequirement
```

```
$st.RelyingParty= '*'
```

```
$st.State= 'Enforced'
```

In addition, we need to specify at least one strong authentication method object:

```
$m1 = New-Object -TypeName Microsoft.Online.Administration.  
StrongAuthenticationMethod
```

```
$m1.IsDefault = $true
```

```
$m1.MethodType = "OneWaySMS"
```

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

These are some of the possible options for MethodType:

- ▶ OneWaySMS: Text code to mobile phone number;
- ▶ TwoWayVoiceMobile: Call my mobile phone;
- ▶ TwoWayVoiceOffice: Call my office phone;
- ▶ TwoWayVoiceAlternateMobile: Call an alternate mobile phone number;
- ▶ PhoneAppOTP: Show a one-time password (OTP) in application; for example, a six-digit number;
- ▶ PhoneAppNotification: Notify me through an app using in-app verification.

You will notice that when end users configure PhoneAppNotification, they will also have the PhoneAppOTP method configured by default, as well as fallback for situations when there is no data coverage. The OneWaySMS, TwoWayVoiceMobile and TwoWayVoiceOffice methods will use the currently configured mobile or office phone number attributes.

```
$m2 = New-Object -TypeName Microsoft.Online.Administration.  
StrongAuthenticationMethod
```

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

```
$m2.IsDefault = $true
```

```
$m2.MethodType = "TwoWayVoiceMobile"
```

To enable end users for Office 365 authentication with MFA using these two contact methods, we configure the user object as follows:

```
Set-MSolUser -UserPrincipalName michel@test.com  
-StrongAuthenticationRequirements @($sta) -StrongAuthentication-  
Methods @($m1, $m2)
```

Over time, administrators may want to see MFA-enabled end users and what contact methods they've configured. MFA-enabled end users have their `StrongAuthenticationRequirements` attribute configured. When they've configured their MFA method, the `StrongAuthenticationMethods` attribute contains the configured method. With this knowledge, we can construct a cmdlet to get a list of MFA-enabled users and the configured methods (Figure 1):

```
Get-MSolUser | Where {$_.StrongAuthenticationRequirements} | Select
```

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

```
UserPrincipalName, @{n="MFA"; e={$_.StrongAuthenticationRequirements.State}}, @{n="Methods";
e={$_.StrongAuthenticationMethods.MethodType}}
```

```
PS C:\> Get-MsOUser | Where { $_.StrongAuthenticationRequirements } | Select UserPrincipalName, @{n="MFA"; e={$_.StrongAuthen
ticationRequirements.State}}, @{n="Methods"; e={$_.StrongAuthenticationMethods.MethodType}}
```

UserPrincipalName	MFA	Methods
andre@...onmicrosoft.com	Enforced	<OneWaySMS, TwoWayVoiceMobile>
nichel@...onmicrosoft.com	Enabled	
roland@...onmicrosoft.com	Enabled	
haarten@...onmicrosoft.com	Enforced	<PhoneAppOTP, PhoneAppNotification, ...>

Figure 1

MFA-enabled administrators have browser-only access. One of the important applications not supporting MFA yet is the PowerShell module, but native support is planned for the later part of 2014. Until that time, MFA-enabled administrators are required to use the Office 365 admin center for only regular management tasks. To run PowerShell cmdlets or scripts in their tenant, administrators should create and use a special-purpose account with a strong password, leaving MFA disabled.

MICHEL DE Rooij is a consultant and Exchange MVP from the Netherlands. Michel started originally as a developer back in 1994 but quickly switched to infrastructure-related projects and started focusing on Exchange in 2004, covering a number of areas, including migrations, transitions, consolidation and disentanglement. Besides Exchange, Michel's other areas of interest are PowerShell, Active Directory,

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

Lync and messaging in general. Michel is a contributor to The UC Architects podcast theucarchitects.com and blogs about Exchange and related subjects at eightwone.com.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

SECURE OFFICE 365 WITH THE CLIENT ACCESS POLICY BUILDER

Steve Goodman

For many organizations, a move to Office 365 brings new options for accessing services, such as Microsoft Exchange, over the Internet. Even though many organizations provide access to Outlook Web App, Outlook Anywhere or ActiveSync, some don't want end users to access email from an Internet cafe, a personal device or anywhere outside the office. If your organization fits into the latter category, you should build a Client Access Policy.

Office 365 is an Internet-based service, which means that unless you buy Microsoft's dedicated offering, all clients must traverse the public Internet to access it. Some organizations mandate client access be from secured (often corporate) devices.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

Out of the box, one advantage of Office 365 is you don't need to be on a corporate device. You can access provided services, including installing Outlook and downloading email, from anywhere with Internet connectivity. For some organizations, especially those that work with financial or personal information, the ability to connect any device this way means they could potentially breach regulations or internal business policies.

For Office 365 to be a viable technology, moving services such as email to it means having the ability to restrict who can access it -- and from where -- as well as what's essential. But it's more complicated than restricting who and what can access the Active Directory Federation Services (AD FS) servers federated with Office 365.

Outlook is an active client, which means the client sends the username and password to Office 365, which then reaches out and authenticates on the end user's behalf. Unless you only want to use basic browser-based services such as OWA and SharePoint, you'll need to provide access to AD FS from Office 365 addresses. By default, any Outlook client with the correct credentials can authenticate whether or not the AD FS servers are exposed to the wider Internet.

Microsoft knows this is a requirement for many organizations, so it built in a feature called Client Access policies.

AVAILABLE FEATURES AND KEY REQUIREMENTS

A Client Access Policy is one of a number of basic policies Microsoft supports for restricting access to Office 365:

- ▶ Block all external access to Office 365 services;
- ▶ Block all external access to Office 365 services, except from ActiveSync devices;
- ▶ Block all external access to Office 365 services, except from passive (e.g., browser-based -- OWA or SharePoint Online) clients;
- ▶ Block all external access to Office 365 services to members of specific Active Directory Groups;
- ▶ Block only external Outlook clients.

When we say "block all external access," this means from IP address ranges you don't specify. If VPN clients access Office 365 through your Internet break-out, they are classified as internal. All of these policies block access to Lync Online and the licensing services for Office 2013 from external clients.

On the server side, you need to make sure you meet two minimum requirements:

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

- ▶ AD FS 2.0 Update Rollup 2, AD FS 2.1 or AD FS 2012 R2;
- ▶ AD FS proxy, Web Application Proxy or a reverse proxy that meets these requirements outlined.

AD FS and the Office 365 tenant should be in a good, working state. This typically means that one or two test mailboxes have been configured and you've tested authentication across clients.

You'll need to choose which of these scenarios best meets your requirements, and make sure you have a complete list of external IP addresses or IP address ranges from which internal clients will come.

IMPLEMENTING A CLIENT ACCESS POLICY

The documentation for Client Access policies on TechNet can seem complex if you're looking to go off the beaten track or build your own regular expressions for IP address ranges. But there's a simpler way to set them up.

By using Microsoft's Client Access Policy Builder, which is a PowerShell script that gives you a graphical user interface, you can implement changes using a helpful wizard. To get started, simply download the script to your primary AD FS server. If you're running Windows Server 2012 R2, you'll need to make

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

a small adjustment to the script before execution to ensure it correctly loads the AD FS module.

Search for the following line:

```
If (($OSVersion.Major -eq 6) -and ($OSVersion.Minor -eq 2))
```

Replace the -eq with -ge so it detects we're running 2012 R2 (minor version 3):

```
If (($OSVersion.Major -eq 6) -and ($OSVersion.Minor -ge 2))
```

We've completed the hard part. Now, launch the Client Access Policy builder. You'll see the builder UI as a simple one-page form. When you're ready to make the changes, locate Step 1 and choose Create Rules for Claim Types (Figure 1).

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

Office 365 - Client Access Policy Builder

Step 1
After the Update Rollup 1 for Active Directory Federation Services (AD FS) 2.0 package has been installed on all federation servers and federation server proxies, and the AD FS Windows service has been restarted, use the following button to add a set of claim rules that make the new claim types available to the policy engine.

Create Rules for Claim Types

Step 2
Choose one of the example scenarios below to configure the claim rules on the Microsoft Office 365 Identity Platform relying party trust that best meets the needs of your organization, enter an external IP address or external IP address range, and click the Build button.

- Block all external access to Office 365
- Block all external access to Office 365, except Exchange ActiveSync
- Block all external access to Office 365, except for browser-based applications such as Outlook Web Access or SharePoint Online
- Block all external access to Office 365 for members of designated Active Directory groups
- Block only external Outlook clients

IP Selection

- Single external IP address . . . Invalid
- External IP address range . . . - . . .

The x-ms-forwarded-client-ip claim is populated from an HTTP header that is currently set only by Exchange Online, which populates the header when passing the authentication request to AD FS. The value of the claim may be a single IPV4 address or a IPV4 address range. Currently, this tool allows only a range in the last octet of the IPV4 address. For more information, click Help.

Help **Build**

Figure 1. Client Access Policy builder

After creating the claim types, enter the settings specific to your scenario. For our example, we'll choose to block all external access except for Exchange ActiveSync, and then enter our organization's external IP address. When we're happy with the new configuration, we'll choose Build (Figure 2).

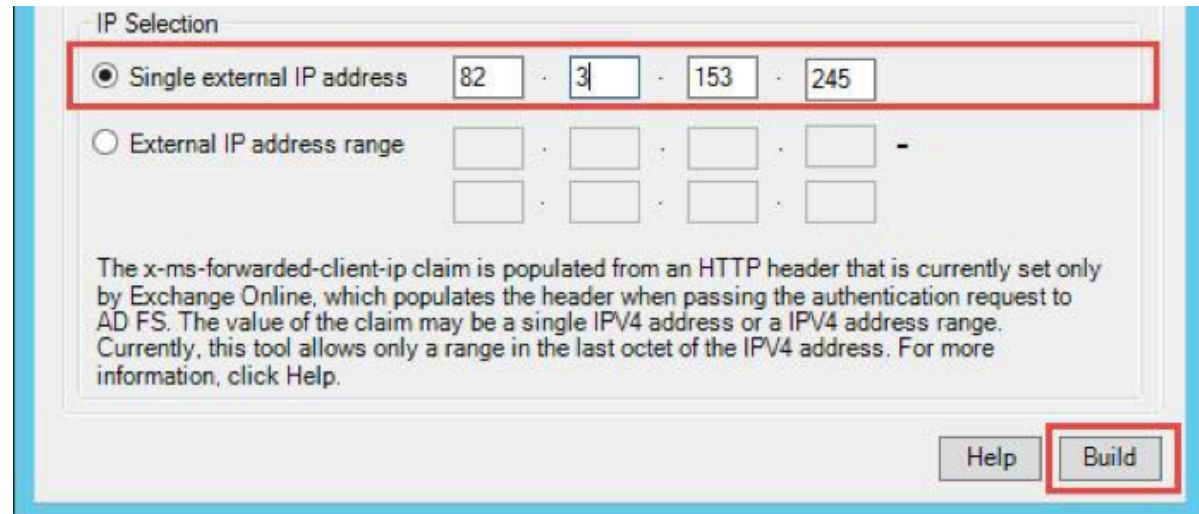


Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder



IP Selection

Single external IP address 82 . 3 . 153 . 245

External IP address range [] . [] . [] . [] -
[] . [] . [] . []

The x-ms-forwarded-client-ip claim is populated from an HTTP header that is currently set only by Exchange Online, which populates the header when passing the authentication request to AD FS. The value of the claim may be a single IPV4 address or a IPV4 address range. Currently, this tool allows only a range in the last octet of the IPV4 address. For more information, click Help.

Help Build

Figure 2. Build claim type.

After making the changes, we can verify they've been applied within the AD FS Management Console. Navigate to Trust Relationships > Claims Provider Trusts and locate Active Directory. Then choose Edit Claim Rules (Figure 3). You'll see five new rules as described in Step 2 of the TechNet article referenced above (Figure 4).

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

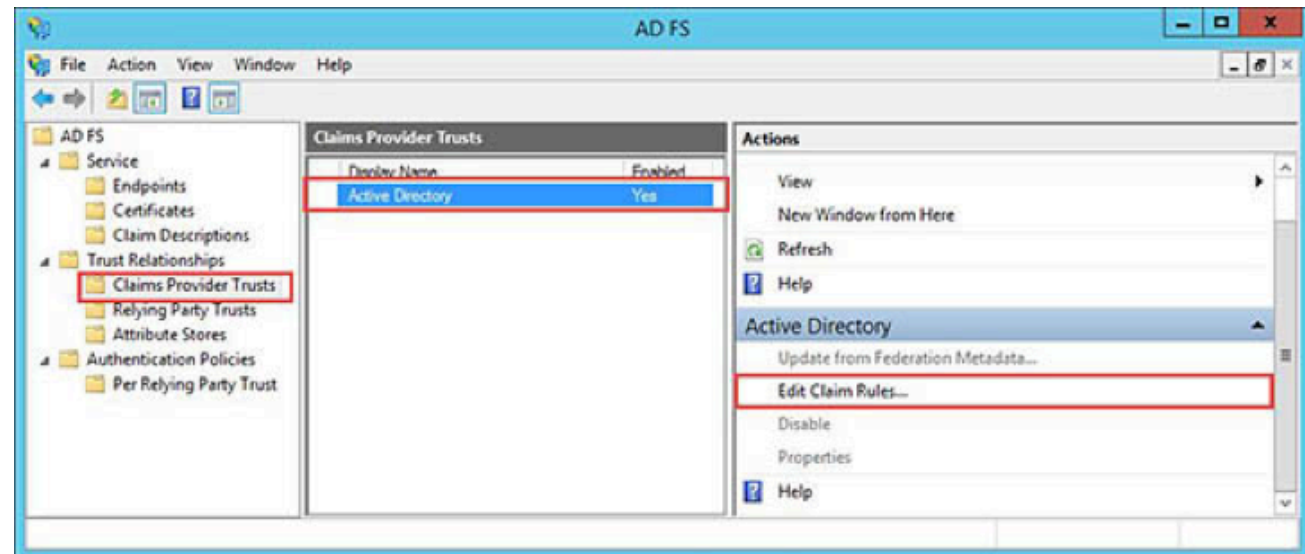


Figure 3. Edit claim rules.

Home

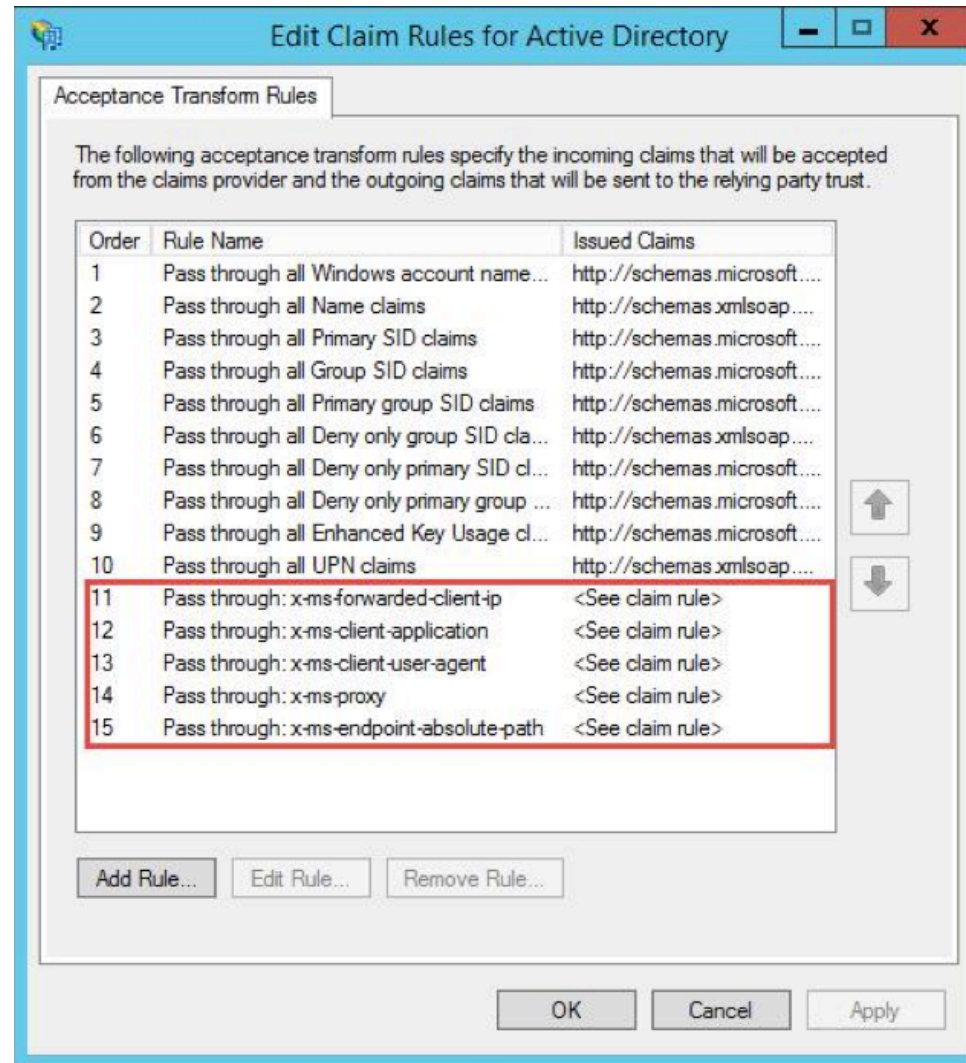
An introduction to
Microsoft Office 365
securityConfigure Office 365
authentication with
PowerShellSecure Office 365
with the Client
Access Policy Builder

Figure 4. New claim rules

Home

An introduction to
Microsoft Office 365
securityConfigure Office 365
authentication with
PowerShellSecure Office 365
with the Client
Access Policy Builder

You can then verify that the rules to block Office 365 access from external clients were applied by navigating to Trust Relationships > Relying Party Trusts then choosing Edit Claim Rules for the Microsoft Office 365 Identity Platform (Figure 5).

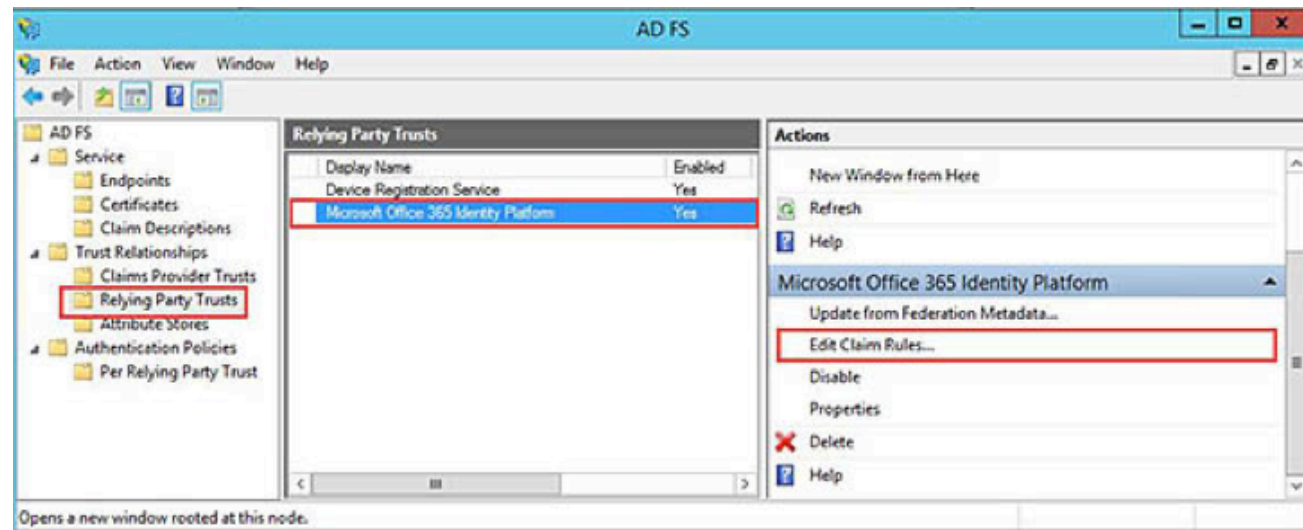


Figure 5. Microsoft Office 365 Identity Platform.

The Edit Claim Rules window should appear. Select Issuance Authorization Rules, check that you have a new claim listed named Block all external access to Office 365 and then choose Edit Rule (Figure 6).

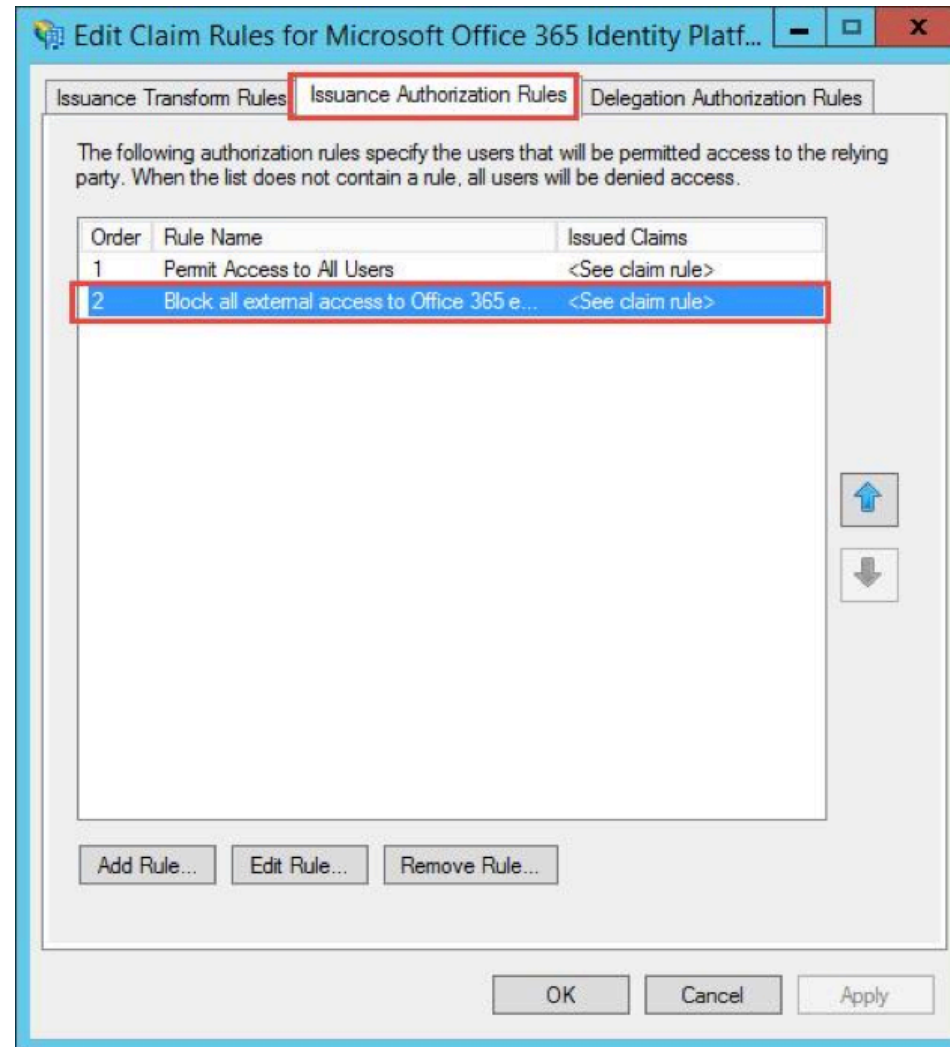


Figure 6. Issuance Authorization Rules.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

You'll see the contents of the rule. ActiveSync is explicitly mentioned, along with the external IP address (Figure 7).

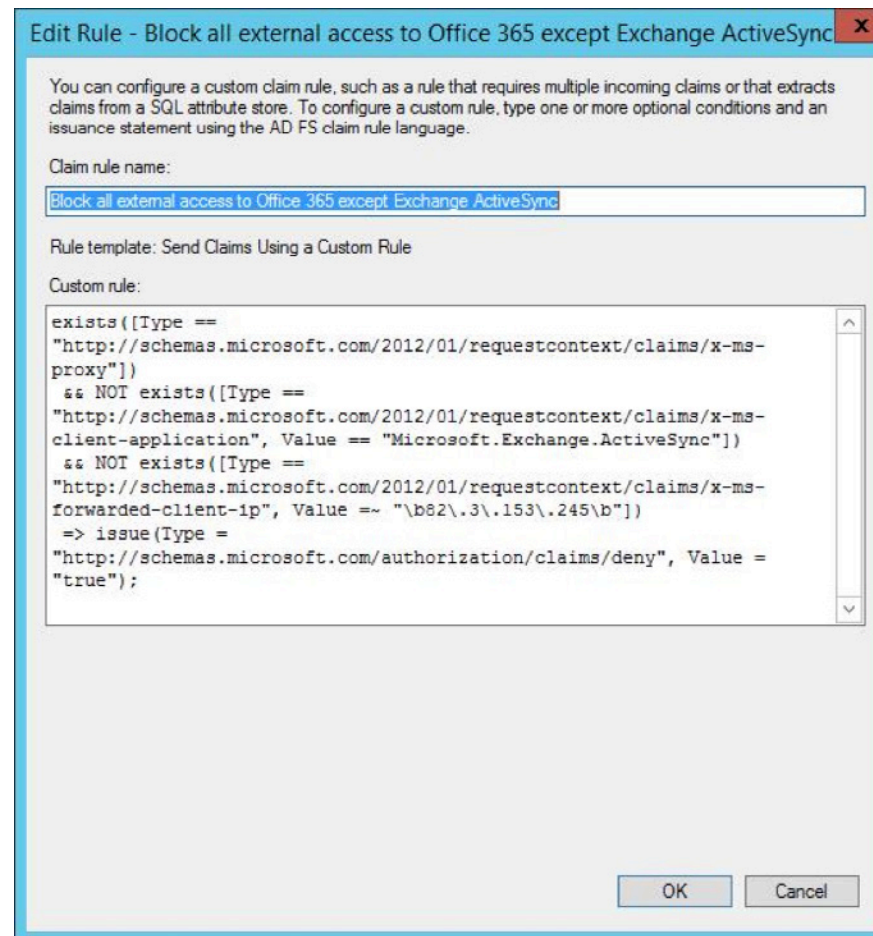


Figure 7. ActiveSync in claim rules.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

You don't need to make any changes to what's here unless you want to delete the new rules.

As with any change, ensure that the AD FS alternations have the expected results. Access from internal clients and Exchange ActiveSync clients should be unaffected. Access from external clients should result in a Not Authorized error message on attempted sign-in using a browser or refusal to accept the password in Outlook.

STEVE GOODMAN is an Exchange MVP, and works as a technical architect for one of the U.K.'s leading Microsoft Gold partners. Goodman has worked extensively with Microsoft Exchange since version 5.5 and with Office 365 since its origins in Exchange Labs and Live@EDU.

Home

An introduction to
Microsoft Office 365
security

Configure Office 365
authentication with
PowerShell

Secure Office 365
with the Client
Access Policy Builder

[Home](#)[An introduction to Microsoft Office 365 security](#)[Configure Office 365 authentication with PowerShell](#)[Secure Office 365 with the Client Access Policy Builder](#)

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.