Securing Office 365 with Okta

okta

Index

Background

As the leading independent provider of enterprise identity, Okta integrates with more than 5500+ applications out-of-the-box. Most of these applications are accessible from the Internet and regularly targeted by adversaries. Okta's security team sees countless intrusion attempts across its customer base, including phishing, password spraying, KnockKnock, and brute-force attacks. They continuously monitor and rapidly respond to these attacks to protect customer tenants and the Okta service. The most commonly targeted application for these attacks is Office 365, a cloud business productivity service developed by Microsoft.

Okta's customers commonly use a combination of single sign-on (SSO), automated provisioning, and multi-factor authentication (MFA) to protect their Office 365 tenants against the aforementioned attacks. However, Office 365 uses several authentication methods and access protocols, including options that do not support MFA in their authentication flow. It has become increasingly common for attackers to explore these options to compromise business email accounts.

This document covers the security issues discussed above and provides illustrative guidance on how to configure Office 365 with Okta to bridge the gap created by lack of MFA for Office 365. This information is based on internal research performed by the Okta security team and does not constitute a replacement for Okta documentation addressing Office 365 configuration for Okta.

Terms & Definitions

Authentication Methods

A. **Basic Authentication**

Basic Authentication, in the Office 365 suite, is a legacy authentication mechanism that relies solely on username and password. It has proven ineffective and is not recommended for the modern IT environments especially when authentication flows are exposed to the internet as is the case for Office 365.

B. **Modern Authentication**

To address the common security concerns and end-user experience requirements associated with Office 365 deployments, Microsoft introduced the Active Directory Authentication Library (ADAL) for Office 365 client applications, referred to as Modern Authentication. Modern Authentication helps secure Office 365 resources using multi-factor authentication, certificate-based authentication, and SAML-based logins (such as federation with Okta), for a true single sign-on experience.

Access Protocols

Office 365 supports multiple protocols that are used by clients to access Office 365. In the context of this document, the term “Access Protocol” indicates the protocols such as POP, IMAP, Exchange ActiveSync, Exchange Web Services (EWS), MAPI and PowerShell. In the context of authentication, these protocols fall into two categories:

A. **Legacy Authentication Protocols**

Protocols like POP and IMAP, which do not support modern authentication methods are referred to as legacy authentication protocols.

B. **Modern Authentication Supported Protocols**

Protocols like, Exchange ActiveSync, EWS, MAPI, and PowerShell, which support both basic and modern authentication methods are classified as modern authentication protocols, in the context of this document.

New Device Access Email Notification

Okta supports a security feature through which a user is notified via email of any sign-on that is detected for their Okta user account from a new device or a browser. The email provides information about the timestamp, location, and device information, such as IP Address and user agent (OS version/browser).

Office 365 Client Access Policies

Okta provides an approach to enable per-application sign-on policy to make access decisions based on group membership, network locations, platform (desktop or mobile), and multi-factor authentication, to name a few. However, with Office 365 client access policies, the access decision can also be implemented based on client type, such as web browser, modern auth or legacy auth clients. For more details refer to Getting Started with Office 365 Client Access Policy.

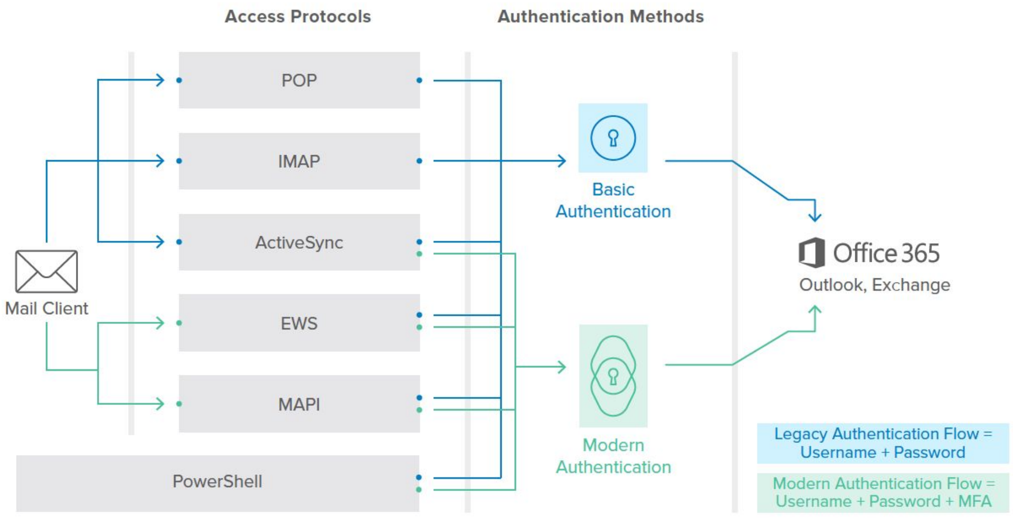
Introduction

Office 365 email access is governed by two attributes: an authentication method and an access protocol. Email clients use a combination consisting of one of each of the two attributes to access Office 365 email. It is important for organizations to be aware of all the access protocols through which a user may access Office 365 email, as some legacy authentication protocols do not support capabilities like multi-factor authentication. Table 1 summarizes the list of Office 365 access protocols and the authentication methods they support.

Access Protocols	Basic Authentication	Modern Authentication
POP	✓	✗
IMAP	✓	✗
Active Sync	✓	✓
EWS	✓	✓
MAPI	✓	✓
PowerShell	✓	✓

Table 1: Protocol and supported authentication methods

Note that 'PowerShell' is not an actual protocol used by email clients but required to interact with Exchange. Figure 1 below shows the Office 365 access matrix based on access protocols and authentication methods listed in Table 1:



Problem Statement

In most corporate environments nowadays, it is imperative to enforce multi-factor authentication to protect email access. Doing so for every Office 365 login may not always be possible because of the following limitations:

A. Not all access protocols used by Office 365 mail clients support Modern Authentication. Protocols like POP and IMAP only support basic authentication and hence cannot enforce MFA in their authentication flow.

B. Regardless of the access protocol, email clients supporting Basic Authentication can sign-in and access Office 365 with only username and password despite the fact that federation enforces MFA.

C. Modern authentication protocols like Exchange ActiveSync, EWS and MAPI can also be used with basic authentication. For example, Outlook clients can default to Basic Authentication when by modifying registry on Windows machines.

D. Office 365 currently does not offer the capability to disable Basic Authentication. Therefore, even if Modern Authentication is enabled on an Office 365 tenant, mail clients can still access it using Basic Authentication.

E. In environments where Okta is used for federation, using legacy authentication protocols (POP and IMAP), that rely on Basic Authentication does not trigger the New Device Access email notification.

This complexity presents a major challenge in balancing support for email applications preferred by end-users and enforcing MFA across the entire Office 365 environment. The “Expected Behavior/Changes” section below addresses the trade-offs that must be made to enforce MFA for Office 365.

Office 365 Authentication Methods

Behind the scenes, Office 365 suite uses Azure AD for handling authentication i.e. an Azure AD instance is bundled with Office 365 license. Azure AD supports two main methods for configuring user authentication:

A. **Cloud Authentication**, using either:

   a. Password Hash Synchronization, or
   b. Pass-through Authentication

B. **Federation**

   Later sections of this paper focus on changes required to enforce MFA on Office 365 using federated authentication with Okta as IDP. However, there are few things to note about the cloud authentication methods listed above.

Password Hash Synchronization relies on synchronizing password hash from an on-premise Active Directory (AD) to a cloud Azure AD instance. This allows users to authenticate to cloud-based services such as Office 365 using the same password as the on-premises AD. In this scenario, **MFA can only be enforced via Azure MFA**, third-party MFA solutions are not supported.

Pass-through Authentication allows users to use the password to access cloud services like Office 365, as the one stored in on-premise AD. Pass-through authentication removes the need to synchronize the password hash to a cloud Azure AD by using intermediate systems called pass-through authentication agents that act as liaison between on-premises AD and Azure AD. It is important to note that MFA can be enforced only via Azure MFA when Pass-through Authentication is used, Third party MFA and on-premises MFA methods are not supported.

Having addressed relevant MFA requirements for the Cloud Authentication method, we can focus on how to secure federated authentication to Office 365 with Okta as Identity Provider in the next sections.

Securing Federated Office 365 Using Okta

Enforcing MFA in Office 365 federated to Okta requires executing a number of steps. Enforcing MFA in this context refers to closing all the loopholes that could lead to circumventing the MFA controls. It is of key importance that the steps involved in this configuration changes are implemented and in the order listed below:

A. **Federate Office 365 authentication to Okta**

B. **Enable Modern Authentication on Office 365**

C. **Disable Legacy Authentication Protocols on Office 365 (OPTIONAL)**

D. **Disable Basic Authentication on Office 365**

E. **Configure Office 365 client access policy in Okta**

F. **Revoke refresh-tokens in exchange**

The order of the steps is important because the final step involves invalidating the current Office 365 tokens issued to users, which should be done after the Office 365 client access policies are set in Okta. This will ensure existing user sessions (both non-modern and modern authentication) are terminated and the new session are on Modern Authentication.

Note that the minimum privileges required on Office 365 and the Okta platform to implement these changes are listed in Table 2:

Platform	**Privilege**
Office 365	Organization Management
Okta	Outlook 2016

Table 2: Required Platform Privilege

Expected Behavior/Changes

Before proceeding further, we should mention that the configuration changes listed in this document will enforce the following behaviors:

A. All access to Office 365 will be over Modern Authentication.

B. Clients that rely on legacy authentication protocols (including, not limited to, legacy Outlook and Skype clients and a few native clients) will be prevented from accessing Office 365. More details on clients that are supported to follow.

C. Clients that support modern authentication protocols, will not be allowed to access Office 365 over basic authentication.

D. Office 365 Administrators will need the Modern Authentication supported PowerShell module to connect to online Exchange.

Figure 2 shows the Office 365 access matrix once configurations are implemented:

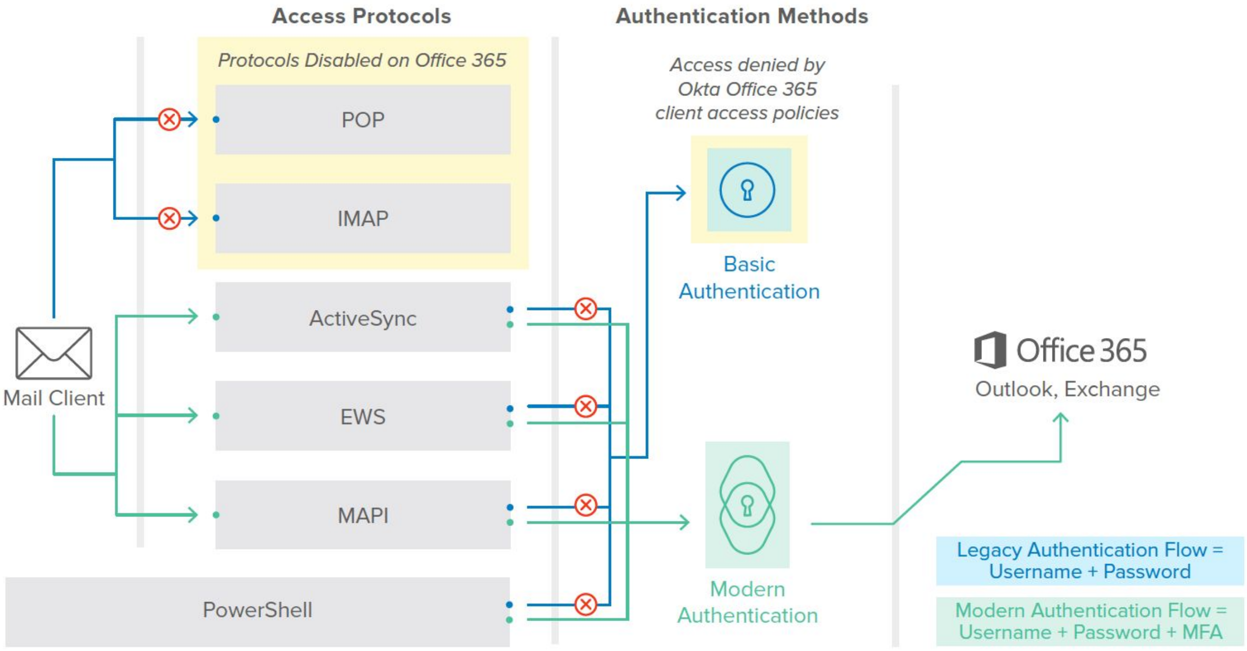

Access Protocols
Authentication Methods
Protocols Disabled on Office 365
POP
IMAP
ActiveSync
EWS
MAPI
PowerShell
Mail Client
Access denied by Okta Office 365 client access policies
Basic Authentication
Modern Authentication
Office 365
Outlook, Exchange
Legacy Authentication Flow = Username + Password
Modern Authentication Flow = Username + Password + MFA

Figure 2: Office 365 Access Matrix after security configuration

Note that, if there is a legitimate business use case for allowing traffic over legacy authentication protocols that rely on Basic Authentication, Office 365 client access policy provides an option to add a user/group exception. The exceptions can be coupled with Network Zones in Okta to reduce the attack surface. An example of a legitimate business use case would be a SaaS integration that uses POP3 or IMAP such as Jira. Organizations can also couple Office 365 client access policy with device trust as a potential solution for managed iOS devices to allow access to Office 365.

A. Federate Office 365 Authentication to Okta

Federated authentication is a method which delegates authentication to the identity provider (IDP), which in this case is Okta. To govern Office 365 authentication with policies defined in Okta, federation needs to be enabled on Office 365. Details about how to configure federation on Office 365 with Okta can be found in Office 365 deployment guide.

B. Enable Modern Authentication

Modern Authentication on Office 365 enables sign-in features such as multi-factor authentication and SAML-based sign-in with Identity Providers, such as Okta. When “Modern Authentication” is enabled in Office 365, clients that support Modern Authentication will use this flow over Basic Authentication.

Modern authentication can be enabled for an Office 365 tenant using PowerShell by executing the following commands:

1. To connect to Office 365 exchange, open Exchange Online PowerShell Module and enter the following command (Replace ‘adminuser@domain’ with the administrator credentials in Exchange):

```
Connect-EXOPSSession -UserPrincipalName @domain>
```

2. Enter the following command to view the current configuration:

```
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

3. If the value of OAuth2ClientProfileEnabled is true, then modern auth is enabled for the domain. If not, use the following command to enable it:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

Note that, because Office 365 does not provide an option to disable Basic Authentication, enabling Modern Authentication alone is insufficient to enforce MFA for Office 365. While newer email clients will default to using Modern Authentication, that default can be overridden by end-users at client-side. Therefore, we also need to enforce Office 365 client access policies in Okta. See section "Configure office 365 client access policy in Okta" for more details.

C. Disable Legacy Authentication Protocols

This is an optional step to ensure legacy authentication protocols like, POP, and IMAP, which only support Basic Authentication, are disabled on Exchange.

The Office 365 Exchange online console does not provide an option to disable the legacy authentication protocols for all users at once. This can be done using the Exchange Online PowerShell Module.

The following commands show how to check users that have legacy authentication protocols enabled and disable the legacy protocols for those users. The commands listed below use POP protocol as an example. You will need to replace 'Pop' in the commands with 'Imap' and 'ActiveSync' to disable those protocols as well.

1. Get a list of all users with POP, IMAP and ActiveSync enabled.

```
Get-CASMailbox -ResultSize Unlimited -Filter
{(RecipientTypeDetails -eq ‘UserMailbox’)} | where
{$_.PopEnabled -eq $true} | FL name
```

2. Disable legacy authentication protocols.

```
Get-CASMailbox -ResultSize Unlimited -Filter
{(RecipientTypeDetails -eq ‘UserMailbox’)} | where
{$_.PopEnabled
-eq $true} | Set-CASMailbox -PopEnabled $false
```

To ensure these legacy authentication protocols are disabled for new users added to exchange, administrators can use SET-CSAMailboxPlan commandlet in PowerShell. Note that this method will only set the configuration for the newly created mailboxes and not the existing ones.

1. List all the Mailbox plans

```
Get-CASMailboxPlan | Select Name,IsDefault
```

2. Disable POP and IMAP

```
Set-CASMailboxPlan -ImapEnabled:$false -PopEnabled:$false
```

D. Disable Basic Authentication on Office 365

In this step, you configure an Authentication Policy in Office 365 to block Basic Authentication. Note that this policy blocks access to legacy protocols at the pre-authentication level, meaning logins coming through legacy endpoints will not be evaluated at all. The Office 365 Exchange online console does not provide an option to disable basic authentication for all users at once. This can be done using the Exchange Online PowerShell Module. The following commands show how to create a policy that denying basic authentication, and how to assign users to the policy.

1. For running Exchange Powershell commands in your windows machine (or server), install the Windows Management Framework 5.1.

```
Connect-EXOPSSession -UserPrincipalName @domain>
```

2. Launch PowerShell as administrator and connect to Exchange:

```
Set-ExecutionPolicy RemoteSigned
$UserCredential - Get-Credential
```

Note: If your administrator account has MFA enabled, follow the instructions in Microsoft's documentation.

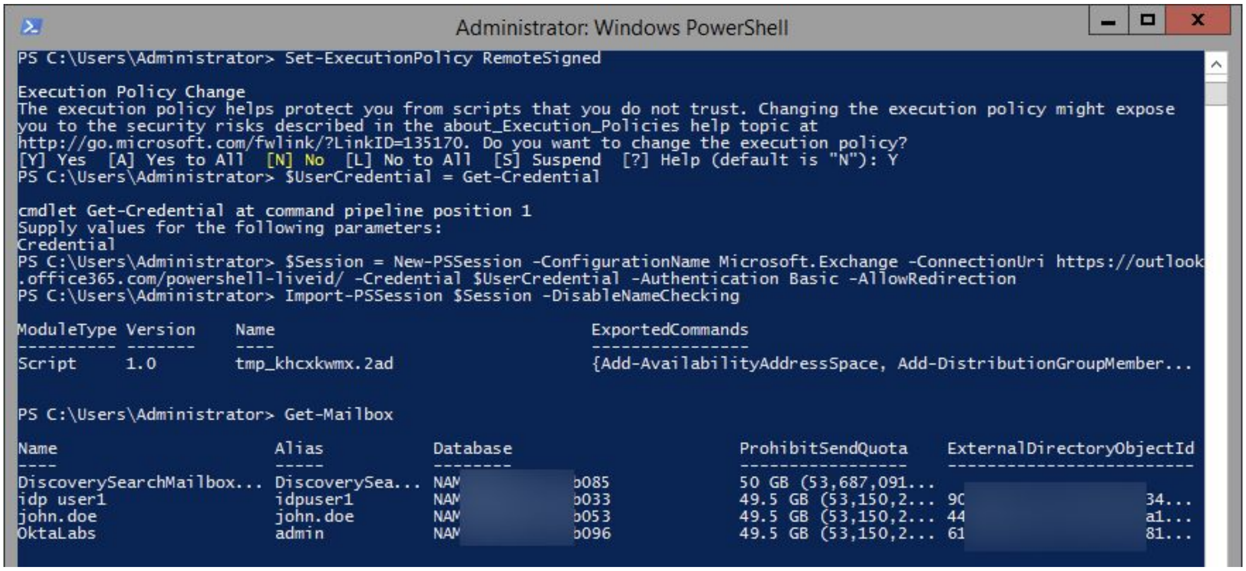
3. Log into your Office 365 Exchange tenant:

```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection

Import-PSSession $Session -DisableNameChecking
```

4. To confirm the connection is completed, enter the command:

```
Get-Mailbox
```

You should see a list of users from your Office 365 tenant:

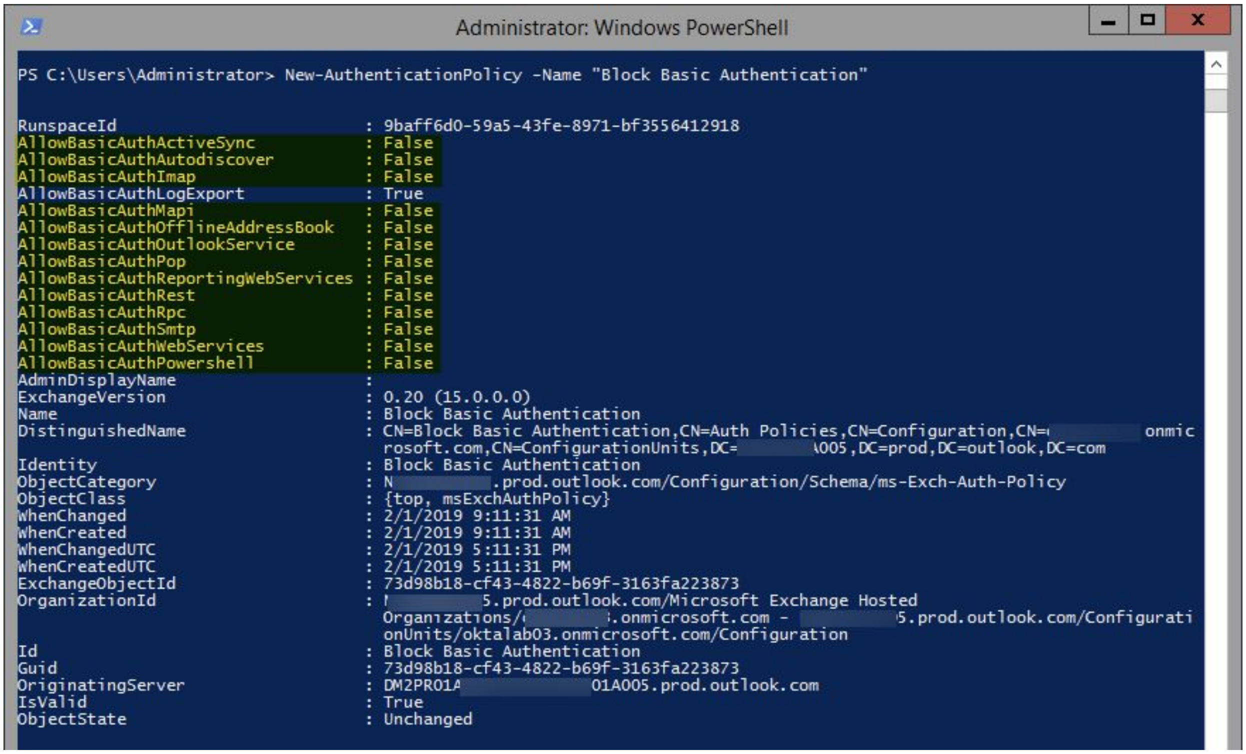


```
PS C:\Users\Administrator> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
PS C:\Users\Administrator> $UserCredential = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Users\Administrator> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook
.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
PS C:\Users\Administrator> Import-PSSession $Session -DisableNameChecking

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     1.0        tmp_khcxkwmx.2ad                    {Add-AvailabilityAddressSpace, Add-DistributionGroupMember...


PS C:\Users\Administrator> Get-Mailbox

Name                      Alias           Database                     ProhibitSendQuota    ExternalDirectoryObjectId
----                      -----           --------                     -----------------    -------------------------
DiscoverySearchMailbox... DiscoverySea... NAM[redacted]b085            50 GB (53,687,091...
idp user1                 idpuser1        NAM[redacted]b033            49.5 GB (53,150,2... 9C[redacted]34...
john.doe                  john.doe        NAM[redacted]b053            49.5 GB (53,150,2... 44[redacted]a1...
OktaLabs                  admin           NAM[redacted]b096            49.5 GB (53,150,2... 61[redacted]81...
```

4. To create an authentication policy denying Basic Authentication, enter the command (this blocks all legacy protocols as mentioned in Microsoft documentation):

```
New-AuthenticationPolicy -Name "Block Basic Authentication"
```

The policy properties are displayed in the terminal. Note that basic authentication is disabled:



```
PS C:\Users\Administrator> New-AuthenticationPolicy -Name "Block Basic Authentication"

RunspaceId                           : 9baff6d0-59a5-43fe-8971-bf3556412918
AllowBasicAuthActiveSync             : False
AllowBasicAuthAutodiscover           : False
AllowBasicAuthImap                   : False
AllowBasicAuthLogExport              : True
AllowBasicAuthMapi                   : False
AllowBasicAuthOfflineAddressBook     : False
AllowBasicAuthOutlookService         : False
AllowBasicAuthPop                    : False
AllowBasicAuthReportingWebServices   : False
AllowBasicAuthRest                   : False
AllowBasicAuthRpc                    : False
AllowBasicAuthSmtp                   : False
AllowBasicAuthWebServices            : False
AllowBasicAuthPowershell             : False
AdminDisplayName                     :
ExchangeVersion                      : 0.20 (15.0.0.0)
Name                                 : Block Basic Authentication
DistinguishedName                    : CN=Block Basic Authentication,CN=Auth Policies,CN=Configuration,CN=[redacted] onmic
                                       rosoft.com,CN=ConfigurationUnits,DC=[redacted]005,DC=prod,DC=outlook,DC=com
Identity                             : Block Basic Authentication
ObjectCategory                       : N[redacted].prod.outlook.com/Configuration/Schema/ms-Exch-Auth-Policy
ObjectClass                          : {top, msExchAuthPolicy}
WhenChanged                          : 2/1/2019 9:11:31 AM
WhenCreated                          : 2/1/2019 9:11:31 AM
WhenChangedUTC                       : 2/1/2019 5:11:31 PM
WhenCreatedUTC                       : 2/1/2019 5:11:31 PM
ExchangeObjectId                     : 73d98b18-cf43-4822-b69f-3163fa223873
OrganizationId                       : [redacted]5.prod.outlook.com/Microsoft Exchange Hosted
                                       Organizations/[redacted].onmicrosoft.com - [redacted]5.prod.outlook.com/Configurati
                                       onUnits/oktalab03.onmicrosoft.com/Configuration
Id                                   : Block Basic Authentication
Guid                                 : 73d98b18-cf43-4822-b69f-3163fa223873
OriginatingServer                    : DM2PR01[redacted]01A005.prod.outlook.com
IsValid                              : True
ObjectState                          : Unchanged
```

6. To confirm that the policy exists – or review the policy, enter the command:

```
Get-AuthenticationPolicy -Identity "Block Basic
Authentication"
```

7. To add assign a user to the policy, use the following command:

```
Set-User -Identity <UserId> -AuthenticationPolicy "Block Basic
Authentication"
```

8. Optionally, apply the policy in 30 minutes (instead of 24 hours) by revoking the user tokens:

```
Set-User -Identity <UserId> -STSRefreshTokensValidFrom
$([System.DateTime]::UtcNow)
```

9. Optionally, use the following PowerShell snippets to assign the authentication policy or clear tokens for multiple users (For more examples, visit Microsoft's documentation):

Example 1: Block users with title containing Engineering

```
$Engineers = Get-User -ResultSize unlimited -Filter
{(RecipientType -eq 'UserMailbox') -and (Title -like
'*Engineering*')}

$EngId = $Engineers.MicrosoftOnlineServicesID

$EngId | foreach {Set-User -Identity $_ -AuthenticationPolicy
"Block Basic Authentication"}

$EngId | foreach {Set-User -Identity $_
-STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

Example 2: Block users from a list:

list.txt contents:

```
john.doe@mydomain.com

jane.doe@mydomain.com
```

PowerShell:

```
$List = Get-Content "C:\temp\list.txt"

$List | foreach {Set-User -Identity $_ -AuthenticationPolicy
"Block Basic Authentication"}

$List | foreach {Set-User -Identity $_
-STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

Example 3: To set the new authentication policy as default for all users:

```
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block
Basic Authentication"
```

E. Configure Office 365 Client Access Policy in Okta

To enforce Office 365 authentication over modern authentication the policies need to be configured in Office 365 application's sign-on section in the Okta Admin console. Specifically, we need to add two client access policies for Office 365 in Okta.

A. Deny access when clients use Basic Authentication and,

B. Enforce MFA on new sign-on/session for clients using Modern Authentication.

These policies are required to ensure coverage when users are not protected by the Office 365 Authentication Policies.

To configure the policies:

1. **In the Okta Admin Console, go to Applications > Office 365 > Sign-on > Sign-on policy**

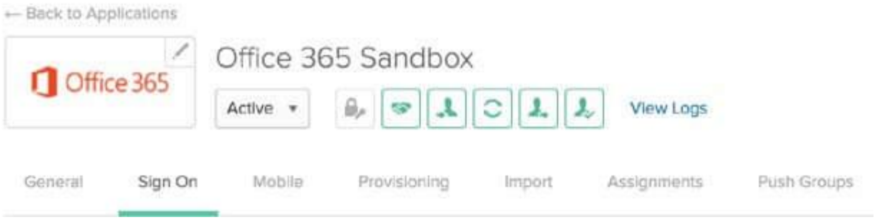


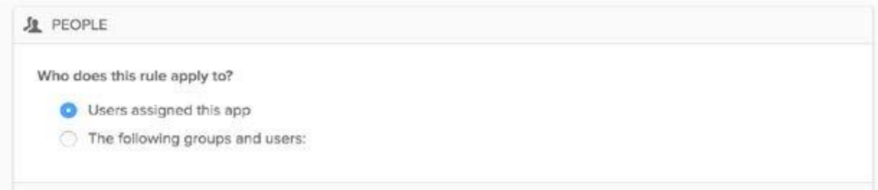
Figure 3: Office 365 Application Configuration in Okta

2. **Create a policy for denying legacy authentication protocols**

The goal of creating a "block" policy is to deny access to clients that rely on legacy authentication protocols which only support Basic Authentication irrespective of location and device platform.

The policy configuration consists of the following:

People: In this section, select all the users/groups that have access to this application.


PEOPLE

Who does this rule apply to?

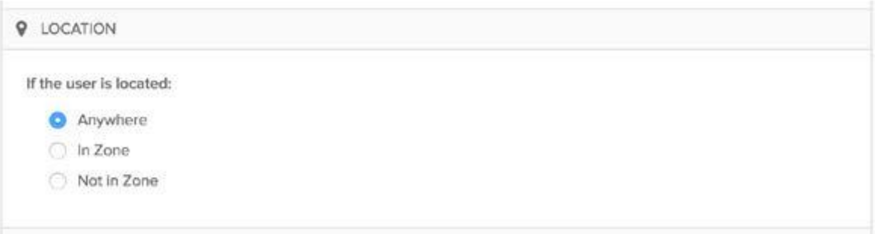
● Users assigned this app

○ The following groups and users:

Figure 4: Office 365 Client Access Policy (Deny) - Part 1

Note: If there is a business requirement for allowing access to legacy authentication protocols, create a group of those user/service accounts and exclude that group from this rule by checking the Exclude the following users and groups from this rule option. For the excluded group, consider creating a separate sign-on policy and allowing restricted access using Network Zones.

Location: Select **Anywhere:**



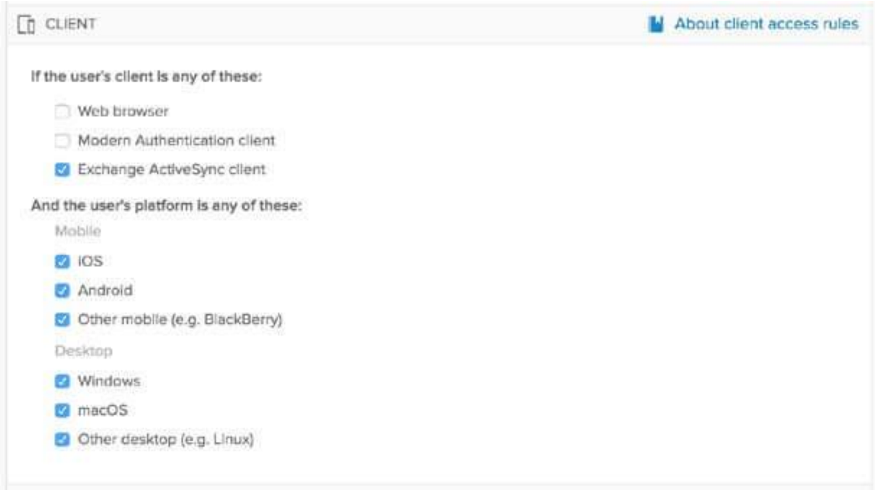
LOCATION

If the user is located:

- ● Anywhere
- ○ In Zone
- ○ Not in Zone

Figure 5: Office 365 Client Access Policy (Deny) - Part 2

Client: In this section, choose "Exchange ActiveSync client" and all user platforms. **This will effectively restrict access based on basic authentication over any access protocol (MAPI, EWS, ActiveSync, POP and IMAP).**



CLIENT

About client access rules

If the user's client is any of these:

- □ Web browser
- □ Modern Authentication client
- ☑ Exchange ActiveSync client

And the user's platform is any of these:

Mobile

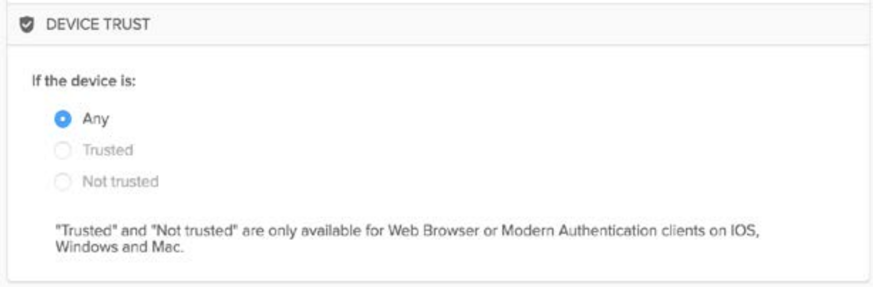
- ☑ iOS
- ☑ Android
- ☑ Other mobile (e.g. BlackBerry)

Desktop

- ☑ Windows
- ☑ macOS
- ☑ Other desktop (e.g. Linux)

Figure 6: Office 365 Client Access Policy (Deny) - Part 3

Device Trust: Choose “Any” i.e. both trusted and non-trusted devices in this section.


DEVICE TRUST

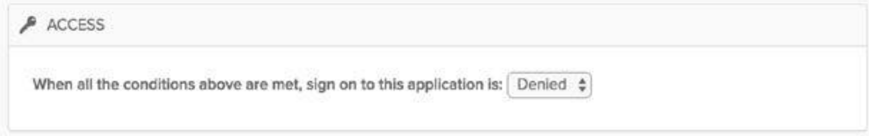
If the device is:

● Any
○ Trusted
○ Not trusted

"Trusted" and "Not trusted" are only available for Web Browser or Modern Authentication clients on IOS, Windows and Mac.

Figure 7: Office 365 Client Access Policy (Deny) - Part 4

Actions: Choose “Denied”


ACCESS

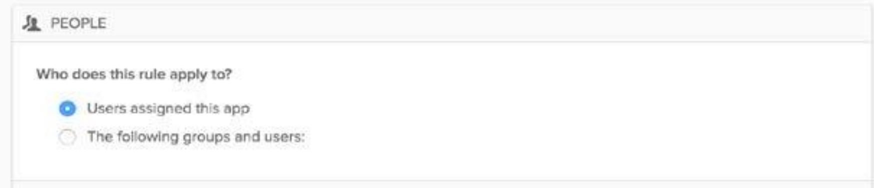
When all the conditions above are met, sign on to this application is: Denied

Figure 8: Office 365 Client Access Policy (Deny) - Part 5

3. **Create a Policy for MFA over Modern Authentication**

The goal of this policy is to enforce MFA on every sign-in to Office 365 application irrespective of location and device platform. The policy configuration consists of the following:

People: In this section, select all the users/groups that have access to this application.

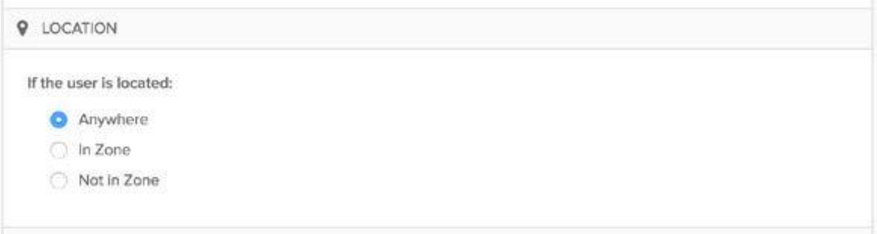

PEOPLE

Who does this rule apply to?

● Users assigned this app
○ The following groups and users:

Figure 9: Office 365 Client Access Policy (Allow) - Part 1

Location: Select **Anywhere:**

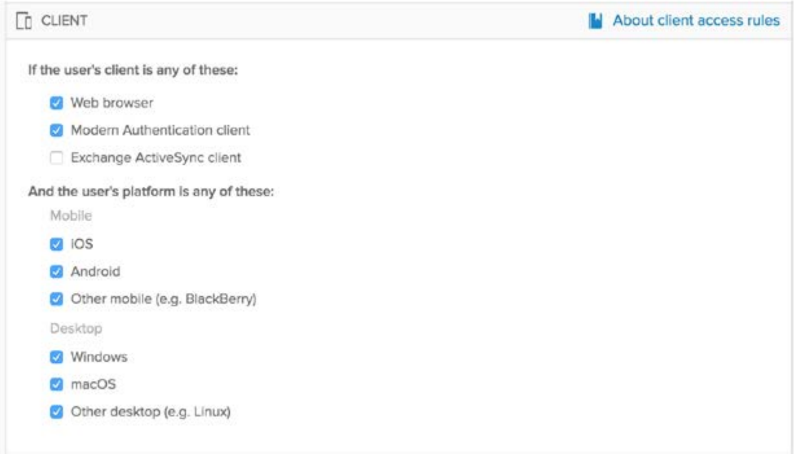

LOCATION

If the user is located:

● Anywhere
○ In Zone
○ Not in Zone

Figure 10: Office 365 Client Access Policy (Allow) - Part 2

Client: Select “Web browser” and “Modern Authentication client” and all platforms:



CLIENT

About client access rules

If the user's client is any of these:

☑ Web browser
☑ Modern Authentication client
□ Exchange ActiveSync client

And the user's platform is any of these:

Mobile

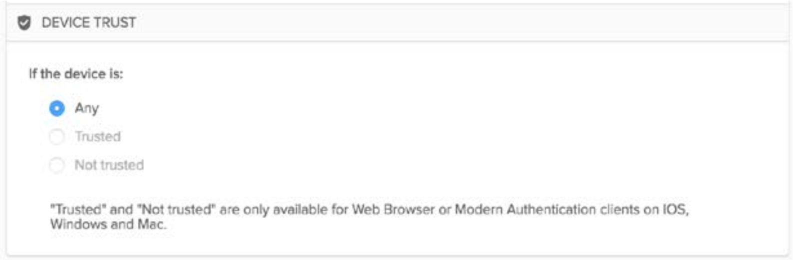
☑ iOS
☑ Android
☑ Other mobile (e.g. BlackBerry)

Desktop

☑ Windows
☑ macOS
☑ Other desktop (e.g. Linux)

Figure 11: Office 365 Client Access Policy (Allow) - Part 3

Device Trust: Choose “Any” i.e. both trusted and non-trusted devices in this section.



DEVICE TRUST

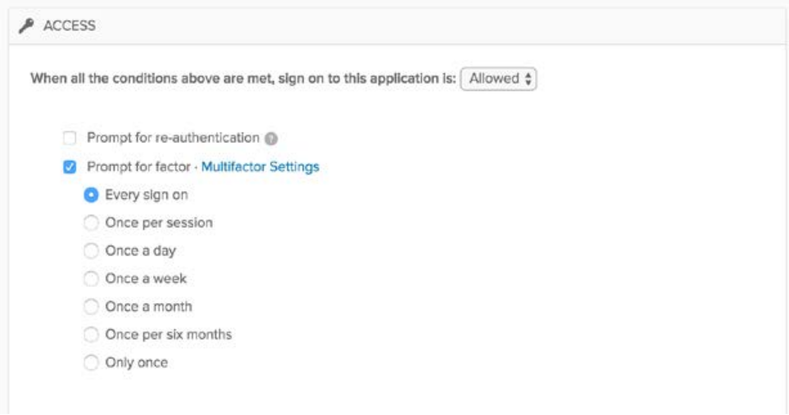
If the device is:

● Any
○ Trusted
○ Not trusted

"Trusted" and "Not trusted" are only available for Web Browser or Modern Authentication clients on IOS, Windows and Mac.

Figure 12: Office 365 Client Access Policy (Allow) - Part 4

Actions: Select “Allowed” and enable “Prompt for factor”. The periodicity of the factor prompt can be set based on the sensitivity of users/groups. For example, if this policy is being applied to high profile users or executives i.e. prompt can be set to every sign-on or every session.



ACCESS

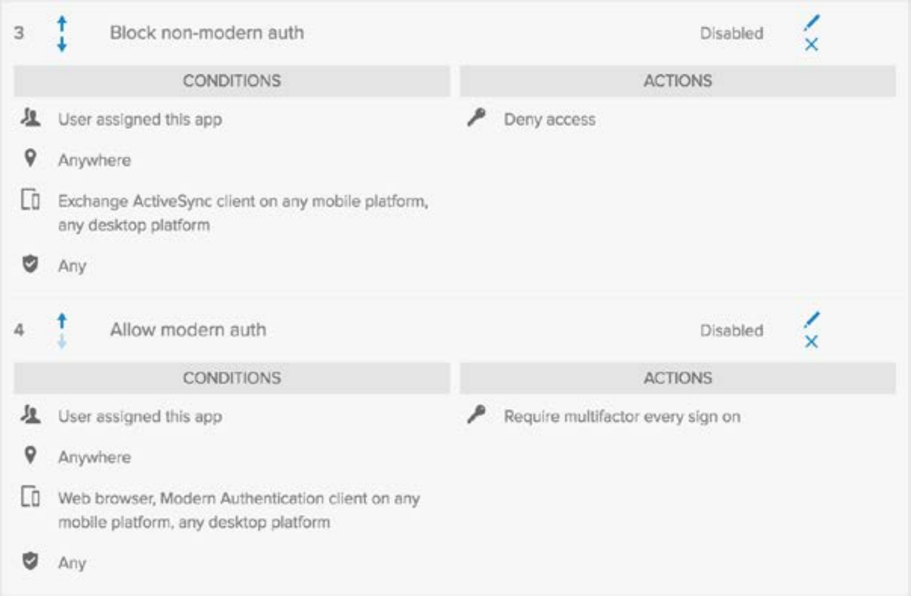
When all the conditions above are met, sign on to this application is: Allowed

□ Prompt for re-authentication
☑ Prompt for factor · Multifactor Settings

● Every sign on
○ Once per session
○ Once a day
○ Once a week
○ Once a month
○ Once per six months
○ Only once

Figure 13: Office 365 Client Access Policy (Allow) - Part 5

Once the above policies in place, the final configuration should look similar to as shown in Figure 14:



3 Block non-modern auth — Disabled

CONDITIONS	ACTIONS
User assigned this app	Deny access
Anywhere	
Exchange ActiveSync client on any mobile platform, any desktop platform	
Any	

4 Allow modern auth — Disabled

CONDITIONS	ACTIONS
User assigned this app	Require multifactor every sign on
Anywhere	
Web browser, Modern Authentication client on any mobile platform, any desktop platform	
Any	

Figure 14: Summary of Office 365 Client Access Policies

F. Revoke Refresh-Tokens

To reduce the number of times a user is required to sign-in to Office 365 application, Azure AD issues two types of tokens i.e. Access and Refresh Tokens. Both tokens are issued when a user logs in for the first time. An access Token is granted for the combination of user, client, and resource that is used when the user first logs in. By default, the Access Token is valid for a period of 1 hour (configurable to a minimum of 10 minutes). Refresh tokens are valid for a period of 90 days and are used to obtain new sets of access/refresh tokens.

Once the user has a valid refresh token, they will not be prompted for login and will continue to have access until the refresh token expires. To ensure that all the configurations listed in previous sections in this document take effect immediately**, refresh tokens need to be revoked.

**** Even after revoking a 'refresh-token', the user might still be able to access Office 365 as long as access token is valid.** Reducing lifetime of access token carries a trade-off between performance and amount of time clients maintain access under the current configuration.

To change the lifetime of an Access Token or revoke a Refresh Token follow the steps mentioned here using PowerShell.

1. Open a new PowerShell window as administrator and Install Azure AD PowerShell Module:

```
Install-Module -Name AzureAD
```

2. To revoke Refresh Token for a single user, log in to exchange using Exchange Online PowerShell Module:

```
Connect-AzureAD

Revoke-AzureADUserAllRefreshToken -ObjectId
```

3. To revoke Refresh Tokens for all users:

```
(Get-AzureADUser).ObjectId | Revoke-AzureADUserAllRefreshToken
```

Known Email Clients that Support Modern Authentication

The official list of Outlook clients that support Modern Authentication, at the time of this publication, is listed in Table 3 and also available on the Microsoft site. These clients will work as expected after implementing the changes covered in this document. The **Outlook Web App** (OWA) will work for all browsers and operating systems as it is browser-based and does not depend on legacy authentication protocols.

Operating System	Native Mail Client
Windows	Outlook 2013 & Outlook 2016
Mac OS	Outlook 2016
Android	Outlook app
iOS	Outlook app
*nix	N/A (*nix platform does not has officially supported Outlook client)

Table 3: Modern Authentication Supported Outlook clients

For a full list of applications (apart from Outlook clients) that support Modern Authentication, see the Microsoft documentation referenced here. To access Exchange Online over Modern Authentication using PowerShell, install the Microsoft Exchange Online Remote PowerShell Module.

Microsoft Outlook clients that do not support Modern authentication are listed below.

Operating System	Unsupported Outlook Client
Windows	Outlook 2010 & lower
Mac OS	Outlook 2011 & lower

Table 4: Outlook clients which do not support modern authentication

List of Email Clients Tested by Okta

Table 5 lists versions of Microsoft Outlook and the operating system native mail clients, that were tested by the Okta Information Security team for Modern Authentication support.

Platform	Native Mail Client	Outlook Client
Windows 10	MailVersion: 17.9126.21785.0	Outlook 2016 Version: 16.0 and above
OSX 10.13.4	Native Mail client does not support modern authentication	Outlook 2016 Version: 16.12 and above
iOS 10.3.3	Native Mail client does not support modern authentication	Outlook Version: 2.75.0 and above
iOS 11.3.1	Native Mail Client (Exchange Discover)	Outlook Version: 2.75.0 and above
Android 8.1.0	Native Mail client does not support modern authentication	Outlook Version: 2.2143 and above
*nix	Native Mail client does not support modern authentication	N/A

Table 5: Outlook and Native clients tested by Okta

Conclusion

By following the guidelines presented in this document, Okta customers can enforce MFA on all mail clients supporting modern authentication, hence helping secure their Office 365 application against phishing, password-spraying, KnockKnock and brute force attacks. Additional email clients and platforms that were not tested as part of this research may require further evaluation.

References

Okta Adaptive MFA

Office 365 Client Access Policies in Okta

App Sign-on Policies in Okta

Network Zones in Okta

Disclaimer

Okta makes this document available to its customers as a best-practices recommendation. This document does not modify or otherwise change Okta's assurances to its customers regarding the security practices Okta employs to secure its Okta, as set forth in Okta's Security & Privacy Documentation, which is online at https://www.okta.com/trustandcompliance/.