Kraft Kennedy

MODERN AUTHENTICATION IN EXCHANGE ONLINE

What you need to know

MODERN AUTHENTICATION IN EXCHANGE ONLINE

What you need to know

Many firms and organizations have come to rely on Exchange Online in the past five years. Not having to worry about on-premises storage and redundancy is often reason enough for many businesses to make the switch to the cloud.

The move to the cloud, however, can bring with it security concerns, as any integrated application must now connect over the internet to the Exchange Online environment, rather than directly to the on-premises Exchange environment you were used to using. That means that even other on-premises applications and scripts need to reach out to the cloud to connect to a user's mailbox.

For years, Microsoft allowed basic authentication to Exchange Online, requiring only a username and password. Now, in order to increase security, Microsoft will no longer allow users to connect to Exchange Online with basic authentication, instead requiring modern authentication, which includes OAuth 2.0.

MODERN AUTHENTICATION VS. BASIC AUTHENTICATION

Why is Microsoft forcing the switch to OAuth? To answer that question, it's important to explain some background first.

For years, Windows and other systems have relied on protocols like CHAP, NTLM and Kerberos, which don't work particularly well over the internet. Authentication for internet resources would typically use basic authentication, which was very simple – username and password were contained in

a single header field, in plain text, Base64 encoding. For this reason, basic authentication needed to be combined with SSL to encrypt the headers – remember: never authenticate to a website that is not SSL protected – and protect the user's credentials.

However, even when HTTPS is used, there are still a number of vulnerabilities for basic authentication. First, the authentication header is sent with each request, so the opportunity to capture credentials is practically unlimited. Second, the password will be cached – and possibly permanently stored – within the browser, creating another avenue of compromise. Additionally, the entire basic authentication process is predicated on a very simplistic and archaic username/password architecture that Microsoft is trying to eliminate.

Enter modern authentication. OAuth is an open standard used for many applications and websites that can grant access to another system's information without a password.

Modern authentication is not a single authentication method, but rather a category of several different protocols that aim to enhance the security posture of cloud-based resources.

Some examples of modern authentication protocols are SAML, WS-Federation and OAuth. While each is different in its execution, all aim to move away from the classic username/password method and rely instead on token-based claims. Therefore, while the user may still provide a username and password for the time being – see more below – those credentials are used to authenticate with an identity provider to generate a token for access. This token has more specific information in the form of a claim that specifies what the requestor does and does not have access to. Tokens expire and can be revoked, increasing the ability to govern access.

Think of entering your home versus a hotel room. When you unlock the front door of your house, you walk in and have access to everything – all the bedrooms, the kitchen, the bathrooms, and every other room. When you're given a

keycard at a hotel, in contrast, you're allowed to get in the front door, your room, maybe the VIP lounge and amenities like the gym. But because of the way the keycard is encoded, you can't access the rooms of other guests, the linen closet or employee-only areas. The hotel keycard may have other properties as well, such as time-based access to certain areas (e.g., the swimming pool is off limits after 9 p.m.). Most important, the keycard can be permanently disabled by the hotel once you've checked out.

Within the cloud, tokens are like your hotel keycard and help govern access to individual resources. These can include Microsoft resources and third-party applications linked to a user's Office 365 identity. The ability to control access is perhaps the most compelling part of the architecture.
If you've ever used your Facebook or Google account to access other websites or apps, you've already experienced the concept.
Tokens may also contain information about more than just your user account, including the current computer or current location, which triggers one of Microsoft's best security tools – Conditional Access. Conditional Access allows organizations to create rules restricting access based on location or device. For example, an organization might choose not to allow access from certain countries or from personal devices.

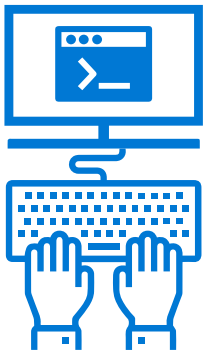
While tokens still require usernames and passwords, the number of instances where you need such credentials has been consistently decreasing, thanks to technologies such as Seamless Single Sign-On, Windows Hello and passwordless authentication with the Microsoft Authenticator app.

ELIMINATING BASIC AUTHENTICATION

How do you stop working through basic authentication when you've relied on it for so long? Elimination starts with identifying and remediating the areas where it's still used.
First, the lowest-hanging fruit: Outlook 2010. Support for modern authentication didn't appear in the Office suite until Office 2013, so if you're still on Office 2010, you're using basic authentication.
If you're planning on moving to Exchange Online, you first need to upgrade your Office applications to a more modern version.

While Outlook 2013 does support modern authentication, it's not enabled

by default, and there are several registry keys that need to be set in order to allow the client to use it. If you're still on Office 2013, enabling modern authentication won't get you off the hook regarding an upgrade – as of October 2020, Office 2013 no longer connects to Office 365 cloud resources such as Exchange Online and OneDrive for Business.



Outlook 2013 and newer clients don't automatically opt out of basic authentication. Modern authentication needs to be specifically enabled within the Exchange Online tenant and can be checked with a simple PowerShell command. After logging into PowerShell for Exchange Online, run the following:

```
Get-OrganizationConfig | FT Name, OAuth2ClientProfileEnabled
```

If the resultant output is "True," then congratulations – you're using modern authentication. If it's "False," you'll need to run the following command to enable it:

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

This will allow clients to use modern authentication and allow you to begin eliminating basic authentication, though it still doesn't prevent its use. The next step is to verify which clients are using basic authentication and to gracefully reconfigure or replace them with applications that support modern authentication.

The best way to do that is to log into the Azure Active Directory portal and navigate to "Sign-ins." You can drill down on the logins and review which users/applications are accessing the portal.

You also need to think about more than just your end users. Anyone who has managed Exchange Online – or any Microsoft product since the late 2000s – knows that trying to do it without PowerShell is like trying to operate with one hand tied behind your back. PowerShell, like Outlook or any other client, needs to authenticate in order to function, and the old method of connecting to Exchange Online via PowerShell used basic authentication. Exchange Online administrators should start working with the EXO V2 PowerShell module, which uses modern authentication and can take advantage of additional security mechanisms such as conditional access and multifactor authentication.

Another quick way to discern the type of authentication

client being used is via the login prompt presented. If your client is requesting credentials, you're still using basic authentication.

WHEN DO YOU NEED TO SWITCH TO OAUTH?

Initially, Microsoft set a cutoff date of October 2020 for basic authentication, but pushed that back to the second half of 2021 due to COVID-19. While this does allow more time for everyone to adjust, it still requires users to reconfigure any applications that integrate with Exchange Online to now use modern authentication, including vendors of third-party applications that integrate with Exchange Online. This may require updates or patches to existing applications, which may in turn require other components to be upgraded or reconfigured.

By summer 2021, you need to be determining which of your applications integrate with Exchange Online and ensuring you have a plan for getting them configured for modern authentication before the deadline arrives. After that date, any application with basic authentication will stop working properly.

NETDOCUMENTS & OAUTH

For organizations that use NetDocuments and have the ndMail application talking to Exchange Online, preparing for OAuth is fairly straightforward. NetDocuments now offers the ability to reconfigure ndMail to leverage OAuth 2.0 instead of basic authentication, and instructions are available online.

The process should take about 5-10 minutes, during which ndMail email filing won't be functional. Instead, it will queue up requests and process messages once the service has been reconfigured. You may want to have administrative access to your Azure portal handy, in case you need to perform any OAuth troubleshooting.

Taking these steps now will allow ndMail filing to continue uninterrupted when Microsoft discontinues basic authentication.

iMANAGE & OAUTH

If you currently have the Work Communications Server for Exchange (WCSE) connected to your Exchange Online environment, iManage has a version that supports modern authentication. In mid-2020,

WCSE 10.2.4 introduced functionality that allowed administrators two options when configuring modern authentication:

1. **App credential flow** – This option uses an SSL certificate and does not require any credentials. It provides impersonation access to all mailboxes in an organization and cannot be limited to a specific subset of users.

2. **User credential flow** – This option leverages a service account with the Application Impersonation role assigned. This option can be scoped only for a certain subset of mailboxes in the organization.

Both options require creating an App Registration in the Azure Portal, so make sure you have your Azure credentials handy. The Administration Guide for WCSE 10.2.4 has detailed instructions on setting this up.

ENDGAME

Once you've eliminated basic authentication from your landscape and have verified that there are no longer any clients attempting to authenticate with legacy protocols to Exchange Online, you can shut the door permanently and restrict basic authentication from your tenant.

Using an authentication policy, you can restrict basic authentication from Exchange Online either on a per-user basis or set it as the default for the entire organization. The best course is generally to do this with a pilot set of users and, assuming there are no issues, eventually expand it to the entire tenant.

The question here is not whether you should restrict basic authentication, but when you'll do it. You want to be well on your way before Microsoft forces the switch to OAuth later this year.

For more information on modern authentication and what your organization needs to do to prepare, contact Kraft Kennedy today.

Contact Us

kraftkennedy.com
hello@kraftkennedy.com
(800) 523-3081