cloudscout.one what's next CW 39

Product: Azure Active Directory

This report contains items, where the 'check before' dates are in the current month and items with upcoming 'check before' dates for the next two months. This is an update-report containing only new or changed items during CW 39.

This is not intended for consumer use. Please respect the work cloudscout.one put into this and don't publish this and respect the copyright. Thank you.

What's next to do Major Items

(Updated) Retirement of IDCRL based sign-in in Office Win32 clients

MC222132

check before:	**09/21/2020**
Status:	
Created:	09/15/2020
Product:	Azure Active Directory, Exchange, Office app, OneNote, Outlook, SharePoint
Platform:	Online, World tenant
Scope:	Security, User, Administration
Ring:	

Updated September 22, 2020: We have updated this post to ensure it is displaying as intended.

Office has introduced a modern and OAuth based authentication mechanism in Office 2016 and Microsoft 365 Apps for enterprise Win32 clients. Modern auth has been the default way of authentication in Office apps since the release of Office 365 ProPlus, more than 4 years ago. We however allowed customers to override this behavior by setting a regkey EnableADAL to 0 so that they could continue to use the legacy form of authentication against Microsoft 365 resources like SharePoint. This legacy form of authentication was powered by a library called IDCRL. It should be noted that the legacy form of authentication for Exchange Online is basic auth, which is different from IDCRL.

Our data suggests that less than 1% of commercial/organization users have overridden the default setting and are still using IDCRL for authentication purposes in Microsoft 365 Apps for enterprise. Modern auth is a more secure way of signing-in. It also allows additional security features like AAD conditional access using multi-factor authentication and device compliance and policies around them.

We are going to remove support for IDCRL library in newer builds of Microsoft 365 Apps for enterprise so that applications like Word, Excel, PowerPoint, OneNote will always use modern authentication with Microsoft 365 resources. This change will not impact Outlook, which uses basic authentication to communicate with Exchange when the EnableADAL regkey is set to 0.

Key points:

Major: Retirement

Timing:

Starting with Current Channel of Microsoft 365 Apps for enterprise version 2010

Semi-Annual Enterprise Channel (Preview) starting version 2102 in March 2021

Semi-Annual Enterprise Channel in July 2021.

Action: No action, this is for awareness

Type: User impact Tenant:

Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support, User Knowledge base
MS Preperations	There is nothing you need to do as this notice is for awareness.
MS How does it affect me	When the change is implemented, users may see a sign-in prompt on each impacted device. Note: this affects only newer builds of Microsoft 365 Apps for enterprise and does NOT impact Office 2016 and 2019 perpetual products.

Seamlessly share personal lists in To Do

MC220931

In MC215678 (June 2020), we announced that Microsoft To Do would support list sharing between personal Microsoft accounts and work or school accounts. We paused the rollout to incorporate your feedback. We are pleased to announce we are moving forward with this feature.
Key points
Microsoft 365 "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=64658" Roadmap ID 64658
Timing: late September
Roll-out: tenant level
Control type: admin control
Action: review and assess by September 25, 2020

check before: **09/25/2020**
Status: **Rolling out**
Created: 08/26/2020
Product: Azure Active Directory, Outlook, To-Do
Platform: Windows Desktop, World tenant, Online
Scope: Administration, UI, User, Compliance, Security
Ring: General Availability, Targeted Release
Type: Admin impact, New feature, User impact
Tenant:

Links	64658,MC215678
Docu to check	User Knowledge base, Working instructions for IT Support
Linked Item Details	MC215678 Title : (Updated) New Feature: Seamlessly Share Personal Lists in To Do MC215678 Url : https://support.office.com/en-us/article/create-and-share-lists-4e5aeac6-8649-4813-aae5-2c2ddea2f292 64658 Title : Microsoft To Do: Support for Sharing Personal Lists 64658 Description: Microsoft To Do will now allow you to share lists from personal to work accounts.
MS Preperations	Once available, this feature will be enabled by default if you have not customized the setting for your tenant. You can manage the feature through Microsoft 365 admin center. You can review the setting in advance and ensure it is set to the experience appropriate for your organization. You can change it at any time; any changes can take up to 24 hours to go into effect. If a user joined a personal (MSA) list when the setting was enabled and you later disable it, the sync between the user and owner will stop within 24 hours. However, the user may continue to see the list for more than 24 hours. You might consider updating your training and documentation as appropriate. How to change the admin setting The admin setting will enable you to restrict people in your organization from joining lists owned by people outside your organization. However, whether or not the setting is enabled, enterprise users will not be able to share their lists with external personal accounts. Go To Microsoft 365 admin center Select Settings in the left hand pane Select Org settings Under Services select Microsoft To Do Select the correct setting in the right-hand fly-out that says “Allow your users to join and contribute to lists shared from outside the organization” Save the settings
MS How does it affect me	A personal Microsoft account (MSA) is an email address used to sign in to Microsoft services like Office 365, Xbox consoles, or Windows 10 PCs. Users can associate any email address as the user name for their MSA, including addresses from Outlook.com, Hotmail.com, Gmail, Yahoo!, or other providers. A work or school account is managed through Azure Active Directory (Azure AD) for a Microsoft 365 tenant. Microsoft To Do will support "https://support.microsoft.com/office/create-and-share-lists-4e5aeac6-8649-4813-aae5-2c2ddea2f292" list sharing between a personal account (MSA) and a work or school account (Azure AD). By default, users in your organization will be able to join, view, modify and add data to lists owned by an MSA. Users in your organization will not be able to share their lists with any account external to your tenant. Nor will users in your organization be able to join, view, modify or add data to lists owned by an external Azure AD account.

(Updated) Prevent/Fix: Updates to on-premises sync-enabled user contact numbers are no longer allowed

MC222474

check before: **09/25/2020**
Status:
Created: 09/19/2020
Product: Azure Active Directory, Graph API
Platform: Developer, World tenant, Online
Scope: Administration, Developer
Ring:

Updated September 24, 2020: We have updated this post with a Blog link for more details.
Starting near the beginning of October, updates to the mobilePhone property of on-premises sync-enabled users will no longer be allowed via Microsoft Graph, Azure AD Graph, or PowerShell. Updates to this property should instead be made in on-premises Active Directory and synced to the cloud. Updates to on-premises sync-enabled objects are not allowed because any changes to these objects are overwritten at the next Azure AD Connect sync cycle, since the source of authority of the objects is on-premises. "https://docs.microsoft.com/en-us/graph/api/resources/user?view=graph-rest-beta#properties" Learn more about which user properties are read-only.

Type: Admin impact, Updated message, User impact
Tenant:

Docu to check	Automation / Scripts
MS Blog Link	https://developer.microsoft.com/en-us/graph/blogs/breaking-change-to-microsoft-graph-users-api-updates-to-on-premises-sync-enabled-user-contact-numbers-are-no-longer-allowed
More Info URL	https://docs.microsoft.com/en-us/graph/api/resources/user?view=graph-rest-beta
MS Preperations	Updates to on-premises sync-enabled user contact numbers properties should instead be made in on-premises Active Directory and synced to the cloud. Please click Additional Information to learn more.
MS How does it affect me	Organizations with apps, scripts, or workflows that use Microsoft Graph or Azure AD Graph to make changes to on-premises sync-enabled user contact numbers will be unable to do so after this change. Microsoft Graph API call before the change Request: PATCH "https://graph.microsoft.com/v1.0/me">https://graph.microsoft.com/v1.0/me Request body: {"mobilePhone": "1112223333" Response: HTTP 204 NoContent Microsoft Graph API call after the change Request: PATCH "https://graph.microsoft.com/v1.0/me">https://graph.microsoft.com/v1.0/me Request body: {"mobilePhone": "1112223333" Response: HTTP 400 Bad Request

```
{
"error": {
"code": "Request_BadRequest",
"message": "Unable to updatethe specified properties for on-premises mastered Directory Sync objects orobjects currently undergoing migration.",
"innerError": {
        "date": timestamp,
        "request-id": request ID,
        "client-request-id": client request ID
```

Prevent/Fix: Shared mailboxes inaccessible due to license expired error

MC222773

check before: **10/01/2020**
Status:
Created: 09/24/2020
Product: Azure Active Directory, Exchange
Platform: Online, World tenant
Scope: Administration
Ring:
Type: Admin impact, User impact
Tenant:

A change was made to Exchange Online to correct the way unlicensed mailbox access is handled. This change may cause Shared mailboxes to be inaccessible due to a license expired error.
Note: If you are not experiencing the following license expired error you can safely disregard this message
"The mailbox isn't available. This may have occurred because the license for the mailbox has expired. To find out how to gain access to this mailbox again, contact the person who manages your email account."

Docu to check	Working instructions for IT Support
MS Preperations	If you are experiencing the error message that the license has expired and the mailbox is showing as a shared mailbox in both On-Prem AD and Azure AD but in Exchange Online it is not a shared mailbox, run the following cmdlet using "https://docs.microsoft.com/powershell/exchange/connect-to-exchange-online-powershell" Exchange Online PowerShell: Set-Mailbox -Type Shared
MS How does it affect me	This could cause delegates who are accessing shared mailboxes to no longer have access. This occurs because both On-Prem AD as well as Azure AD see the mailbox as Shared, but Exchange Online still sees the mailbox as a User mailbox.

What's next to do normal Items

Microsoft 365 admin center: New Microsoft 365 admin center multi-tenant management experiences

67130

check before: **08/31/2020**
Status: **Rolling out**
Created: 09/21/2020
Product: Azure Active Directory, Microsoft 365 admin center
Platform: World tenant, Web, Online
Scope: Administration
Ring: General Availability
Type: Admin impact, New feature
Tenant:

These experiences are for Microsoft 365 admins that manage multiple tenants. They include a tenant switcher, assessing the health and status of multiple tenants, performing repetitive tasks against multiple tenants, and understanding configuration differences between multiple tenants.

Docu to check	Working instructions for IT Support, Service Description

Microsoft Whiteboard introduces per user licensing

MC222821

check before:	**10/01/2020**
Status:	**In development**
Created:	09/25/2020
Product:	Azure Active Directory, Whiteboard
Platform:	World tenant, Online
Scope:	Administration, User, Licensing
Ring:	General Availability
Type:	Admin impact, New feature, User impact
Tenant:	

Microsoft Whiteboard, which is automatically enabled for most Microsoft 365 tenants, will soon read licenses at a user level. There’s no change to how Microsoft Whiteboard is managed at the tenant level. If you do not use Whiteboard in your tenant, you can disregard this message.
This message is associated with Microsoft 365 "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=66761" Roadmap ID 66761.
When this will happenThis feature will be enabled mid-October.

Links	66761
Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support
Linked Item Details	66761 Title : Whiteboard: Per user licensing 66761 Description: Tenant admins will be able to use licenses to enable or disable access to Whiteboard at an individual user level, instead of only at the global tenant level. These licenses currently exist in tenants today, but are not used for enablement.
MS Preperations	There is no change to your current Microsoft Whiteboard tenant setting. User licenses are enabled by default. If you wish to use per user licensing, "https://docs.microsoft.com/azure/active-directory/fundamentals/license-users-groups" you can assign or remove licenses in the Azure Active Directory portal. Learn more: "https://support.microsoft.com/office/enable-microsoft-whiteboard-for-your-organization-1caaa2e2-5c18-4bdf-b878-2d98f1da4b24" enable Microsoft Whiteboard for your organization.
MS How does it affect me	We are introducing the ability to control access to Whiteboard at the user level. These licenses currently exist in tenants, but they have not used for enablement. With this change, Whiteboard will read licenses at both the tenant and user level and will block individual access should you disable a user license.

Optimize your end user experience using reauthentication best practices

MC222813

check before:	**10/01/2020**
Status:	
Created:	09/25/2020
Product:	Azure Active Directory, Office app
Platform:	World tenant, Online
Scope:	Administration, Security
Ring:	

We have recently updated the "https://docs.microsoft.com/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication" target="_blank" style="">remember Multi-Factor Authentication (MFA) on a trusted device feature to extend authentication for up to 365 days. You are receiving this email because you are currently using this setting within your tenant. However, you also have Azure Active Directory (Azure AD) Premium licenses, which allow you to use the "https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency" Conditional Access – Sign-in Frequency policy that provides more flexibility for reauthentication settings.
When this will happen The extended duration for remember MFA on a trusted device and the Conditional Access sign-in frequency policy are available now.

Type:	Admin impact, Feature update, User impact	Tenant:

Docu to check	Automation / Scripts, Working instructions for IT Support
MS Preperations	To get started, review our "https://docs.microsoft.com/azure/active-directory/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime" latest guidance on optimizing the reauthentication experience. Then review your tenant configuration. If you have enabled more than one setting in your tenant, we recommend using only the Conditional Access policies of "https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency" user sign-in frequency or "https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#persistence-of-browsing-sessions" persistent browser sessions. Review "https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime" Configure authentication session management with Conditional Access Review "https://docs.microsoft.com/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication" Remember Multi-Factor Authentication on a trusted device setting
MS How does it affect me	For the optimal user experience, we recommend using "https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency" Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to the remember MFA on a trusted device setting. If using remember MFA on a trusted device, be sure to extend the duration to 90 or more days.

View app permissions and grant admin consent in the Microsoft Teams admin center

MC222892

check before:	**10/03/2020**
Status:	**In development**
Created:	09/26/2020
Product:	Azure Active Directory, Graph API, Microsoft 365 admin center, Teams
Platform:	Developer, World tenant, Online
Scope:	Administration, Developer, Security, IT-Governance
Ring:	Preview
Type:	Admin impact, New feature, User impact
Tenant:	

We are making it easier for IT admins to review, manage, and grant consent to app permissions.
 This message is associated with Microsoft 365 "https://www.microsoft.com/microsoft-365/roadmap?rtc=1&filters=&searchterms=67140" Roadmap ID 67140.
 When this will happen This feature be available in the Teams admin center the end of September.

Links	67140,MC218561
Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support
Linked Item Details	MC218561 Title : (Updated) Introducing resource-specific consent for Microsoft Teams 67140 Title : Microsoft Teams: View app permissions and grant admin consent in the Microsoft Teams admin center 67140 Description: In Teams admin center global admins will be able to review and grant consent to Graph API permissions registered in Azure Active Directory, on behalf of the entire tenant for the permissions an app is requesting such as reading information stored in a team or sending an email on behalf of users. IT admins will also be able to review resource-specific consent (RSC) permissions for the apps within Teams admin center. With that admins will be able to unblock their users for the third-party apps they have already reviewed and approved to use in their organization.
MS Preperations	Learn more: "https://docs.microsoft.com/MicrosoftTeams/app-permissions-admin-center" View app permissions and grant admin consent in the Microsoft Teams admin center
MS How does it affect me	We are announcing three changes in the Teams admin center: Global admins will be able to review and grant consent to Graph API permissions registered in Azure Active Directory on behalf of the entire tenant for the permissions an app is requesting, such as reading information stored in a team or sending an email on behalf of users. Admins will be able to unblock third-party apps they have already reviewed and approved to use in their organization. In July (MC218561) we released the "https://docs.microsoft.com/en-us/microsoftteams/platform/graph-api/rsc/resource-specific-consent" resource-specific consent (RSC) permissions model which granted team owners the ability to consent for an application to access and/or modify a team's data. With this change, IT admins will be able to review the permissions for RSC apps deployed by team owners. IT admins can install apps with team scope to any team in their organization.

● ● ● ● ● ● ● ● ● ●

What's next to do minor Items

CAUTION New item - "Launched"

Manage Windows 10 Enterprise Windows Virtual Desktop VMs with Microsoft Endpoint Manager (MEM)

70742

IT Pros can manage Active Directory or hybrid Azure Active Directory joined Windows 10 Enterprise Windows Virtual Desktop VMs with Microsoft Endpoint Manager (MEM).

check before:	**08/31/2020**
Status:	**Launched**
Created:	09/22/2020
Product:	Azure Active Directory, Windows 10, Windows Virtual Desktop
Platform:	Windows Desktop, World tenant
Scope:	MDM, Administration, Security
Ring:	General Availability
Type:	New feature
Tenant:	

Docu to check Working instructions for IT Support

Manage Windows 10 Enterprise multi-session Windows Virtual Desktop VMs with Microsoft Endpoint Manager (MEM)

70743

IT Pros can manage Active Directory or hybrid Azure Active Directory joined Windows 10 Enterprise multi-session Windows Virtual Desktop VMs with Microsoft Endpoint Manager (MEM).

check before:	**08/31/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Azure Active Directory, Windows 10, Windows Virtual Desktop
Platform:	iOS, Windows Desktop, World tenant
Scope:	Administration, MDM
Ring:	Preview
Type:	Admin impact, Feature update
Tenant:	

Docu to check Service Description, Automation / Scripts

Microsoft Teams: Native Teams authentication for PVA bots

68765

Maker can customize bots to provide personal content knowing which user is interacting with the bot. Contextual awareness of user - knows that "John Smith" is asking the question to the bot.

check before:	**10/31/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Teams, Azure Active Directory
Platform:	World tenant, Online
Scope:	Developer, Administration, IT-Governance
Ring:	General Availability

Type: New feature Tenant:

Docu to check Working instructions for IT Support