cloudscout.one what's next CW 39

Scope: Security

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) Microsoft Information Protection: Exact Data Match will add support for salt

MC220037

Updated September 24, 2020: We are pleased to announce that this is available for all Standard organizations as applicable. We are in the progress of rolling this out for Government customers. Please see the updated timeline below. Thank you for your patience.

Soon, "https://techcommunity.microsoft.com/t5/microsoft-security-and/new-exact-data-match-edm-classification-helps-you-better-detect/ba-p/793526" Exact Data Match (EDM) will support salt in the data hashing process to improve data security.

Key points

Microsoft 365 Roadmap ID: "https://www.microsoft.com/microsoft-365/roadmap?filters=featureid=65207" 65207

Timing:Standard - Complete

Government - Complete by early October

Action: review and assess

check before:	**08/14/2020**
Status:	**Rolling out**
Created:	08/08/2020
Product:	Microsoft Information Protection
Platform:	Web, World tenant, Online
Scope:	Compliance, Security, User, Administration
Ring:	General Availability
Type:	Admin impact, New feature, Updated message
Tenant:	

Links	65207
Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support
Linked Item Details	65207 Title : Microsoft Information Protection: Exact Data Match will support SALT in the data hashing process to improve data security 65207 Description: Exact Data Match will support SALT in the data hashing process to improve data security. Adding a random string, known as a SALT, to each data value prior to hashing can make it much more challenging for an attacker to reverse engineer the original values.
MS Preperations	Once the feature is available, "https://docs.microsoft.com/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification#set-up-the-edm-upload-agent" download and install the appropriate updated EDM Upload Agent (Commercial/GCC, GCC-High, or DoD). Updated Upload Agents will be available when the feature reaches GA. If you had previously hashed, indexed, and uploaded data to the EDM service and are already using EDM and would like to add salt to that hashed data, you will need to re-hash and re-upload that data using the instructions provided on the EDM page. Learn more: "https://techcommunity.microsoft.com/t5/microsoft-security-and/exact-data-match-upcoming-news/ba-p/1492842" Exact Data Match Upcoming News "https://techcommunity.microsoft.com/t5/microsoft-security-and/implementing-microsoft-exact-data-match-edm-part-1/ba-p/1345360" Implementing Microsoft Exact Data Match "https://techcommunity.microsoft.com/t5/microsoft-security-and/microsoft-information-protection-and-compliance-webinar-page/ba-p/1184481" Webinar: Exact Data Match (EDM) classification ("https://aka.ms/MIPC/Video-EDMwebinar" video | "https://aka.ms/MIPC/Blog-EDMWebinar" deck/FAQ)
MS How does it affect me	Adding a random string, known as a salt, to each data value prior to hashing can make it much more challenging for an attacker to reverse engineer the original values. Customers can choose to use a custom salt or a random salt that is generated by Microsoft. The data hashed and uploaded for EDM will be more secure through the addition of the salt to the hashing process.

Microsoft Information Protection: Double Key Encryption

64646

Currently available in preview to Commercial tenants, Double Key Encryption from Microsoft allows you to protect your highly sensitive data while maintaining full control of your key. You can protect your data with two keys - your Azure key and your key in the Double Key Encryption service.

check before:	**08/31/2020**
Status:	**In development**
Created:	07/21/2020
Product:	Microsoft Information Protection
Platform:	Online, World tenant
Scope:	Compliance, Security, Administration
Ring:	General Availability
Type:	New feature, Admin impact
Tenant:	

Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support, User Knowledge base

SharePoint: General Availability of SharePoint Syntex

67134

Microsoft SharePoint Syntex uses advanced AI and machine teaching to amplify human expertise, automate content processing, and transform content into knowledge. SharePoint Syntex will be available as a user-based add-on for Microsoft 365 plans and will be generally available to Microsoft 365 commercial customers on October 1, 2020.

check before:	**08/31/2020**
Status:	**Rolling out**
Created:	09/22/2020
Product:	SharePoint
Platform:	World tenant, Online, Web
Scope:	AI, User, Licensing, Administration, Security
Ring:	General Availability

Type:	New feature, Admin impact, User impact	Tenant:

Docu to check	Service Description, Automation / Scripts, User Knowledge base, User Trainings, Working instructions for IT Support
More Info URL	https://aka.ms/SharePointSyntex/announce

(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

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:	

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

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.

Reminder: Prepare for MDATP for Mac system extensions activation on macOS 11 Big Sur

MC222467

check before:	**09/25/2020**
Status:	
Created:	09/19/2020
Product:	Defender
Platform:	Mac, World tenant
Scope:	Administration, Security
Ring:	

Note: this message applies only to organizations with macOS devices in their environments.

As originally communicated in MC218792 (July '20), when Apple announces general availability of macOS 11 Big Sur, Microsoft Defender ATP for Mac will activate a new system extension-based code path on all Mac devices protected by MDATP. The new code path will be activated immediately after devices upgrade to macOS 11 Big Sur.

Between now and macOS Big Sur general availability, you can evaluate the new MDATP for Mac implementation on Catalina devices that are registered for InsiderFast update channel.

The new code path can be activated on InsiderFast devices running macOS version 10.15.4 or later.

To ensure that the new Microsoft Defender ATP for Mac remains functional and effective immediately after device upgrade to macOS 11 Big Sur, a new remote configuration must be deployed to all macOS devices before Apple announces general availability of macOS 11 Big Sur. If the configuration is not deployed prior to Big Sur GA announcement, immediately after upgrade to Big Sur end-users will be presented with a series of system dialogs asking to grant MDATP agent all necessary permissions associated with the new system extensions.

Key Points:

TimingThe new configuration is available now.

MDATP for Mac's new code path can be evaluated now on Catalina devices in the InsiderFast update channel.

Action: Review and prepare ahead of Apple announcing the macOS 11 Big Sur general availability.

Type:	Admin impact, User impact	Tenant:

Links	MC218792
Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support
Linked Item Details	MC218792 Title : MDATP for Mac is moving to use system extensions instead of kernel extensions
MS Blog Link	https://techcommunity.microsoft.com/t5/microsoft-defender-atp/microsoft-defender-atp-for-mac-is-moving-to-system-extensions/ba-p/1608736
More Info URL	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-sysext-preview
MS Preperations	Review the steps below and assess the impact on your organization: Deploy the specified remote configuration to all macOS devices before Apple announces general availability of macOS11 Big Sur. Deploying configuration proactively across the entire macOS fleet will ensure that even down-level devices are prepared for the day when Apple releases macOS 11 Big Sur and will ensure that Microsoft Defender ATP for Mac continues protecting all macOS devices regardless OS version they were running prior to the Big Sur upgrade. Refer to this documentation for detailed configuration information and instructions: "https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-sysext-policies" New configuration profiles for macOS Catalina and newer versions of macOS Evaluate public preview of MDATP for Mac new implementation on several Catalina devices that are running macOS version 10.15.4 or later and are registered for InsiderFast update channel. To start the preview, refer "https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-sysext-preview">to MDATP for Mac system extensions preview documentation. Monitor Apple’s announcements for macOS 11 Big Sur general availability announcement.
MS How does it affect me	To ensure that Microsoft Defender ATP for Mac remains functional and effective immediately after device upgrade to macOS 11 Big Sur, a new remote configuration must be deployed to all macOS devices before Apple announces general availability of macOS 11 Big Sur. If the configuration is not deployed prior to Big Sur GA announcement, immediately after upgrade to Big Sur end-users will be presented with a series of system dialogs asking to grant MDATP agent all necessary permissions associated with the new system extensions.

Announcing general availability of Microsoft Compliance Manager

MC222638

check before: **09/29/2020**
Status: **Rolling out**
Created: 09/23/2020
Product: Compliance Score, Microsoft Compliance center
Platform: World tenant, Online
Scope: Administration, Compliance, Licensing, Security
Ring: General Availability

As announced at Ignite, Compliance Manager (formerly Compliance Score) is moving out of public preview and the tasks you previously found in Compliance Manager (via the "https://docs.microsoft.com/microsoft-365/compliance/get-started-with-service-trust-portal" Service Trust Portal) are now housed within the Microsoft 365 compliance center under Compliance Manager. We announced the public preview of Compliance Score in November 2019.
This message is associated with Microsoft 365 "https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=searchterms=60771" Roadmap ID 60771.
When this will happenRollout will begin in mid-September and is expected to be complete by the end of September.

Type: Admin impact, New feature
Tenant:

Links	60771
Docu to check	Working instructions for IT Support, User Knowledge base
Linked Item Details	60771 Title : Microsoft Compliance Manager general availability 60771 Description: Compliance Manager is the next generation of the existing Compliance Manager and Compliance Score solutions, which have been in public preview since November 2019. With this announcement, we are consolidating the functionality of these two solutions into one single solution, Compliance Manager, which sits in the Microsoft 365 compliance center. With Compliance Manager, you will benefit from intuitive end-to-end compliance management, a vast out-of-the-box assessment template library and built-in automation to scale your compliance across global, industrial and regional standards.
MS Preperations	Learn more about the benefits of Compliance Manager and "https://docs.microsoft.com/microsoft-365/compliance/compliance-manager" review Compliance Manager technical documentation for setup and implementation guidance. New licensing terms will be going into effect with general availability of the solution. "https://docs.microsoft.com/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#compliance-manager" Review the Microsoft 365 licensing guidance for security and compliance to see what is available for your subscription level. Visit the "http://compliance.microsoft.com/" Microsoft 365 compliance center to begin using the new Compliance Manager experience.
MS How does it affect me	Compliance Manager consolidates the functionality of Compliance Score and Compliance Manager preview solutions. You can see your compliance score, add a template and assessment, and manage improvement actions. You'll see some updates to your visual experience in the Microsoft 365 compliance center as these solutions are now housed within the same portal. Any existing assessments created during the public preview of Compliance Score will continue to be available for use.

Reminder: Retirement of legacy eDiscovery tools

MC222624

check before:	**10/01/2020**
Status:	
Created:	09/23/2020
Product:	eDiscovery, Exchange, Microsoft 365 admin center, Microsoft Compliance center
Platform:	Online, World tenant
Scope:	Administration, Compliance, Security, User
Ring:	

As originally announced in MC200104 (January '20) we will be retiring legacy eDiscovery tools soon.
When this will happen
There are several key dates for this retirement and we're now approaching the October 1, 2020 milestone.
In-Place eDiscovery and Holds in the Exchange admin center (EAC)
 July 1, 2020: You won't be able to create new searches and holds, but you can still run, edit, and delete existing searches at your own risk. Microsoft Support will no longer provide assistance for In-Place eDiscovery Holds in the EAC.
 October 1, 2020: The In-Place eDiscovery Holds functionality in the EAC will be placed in a read-only mode. This means you'll only be able to remove existing searches and holds.
*-MailboxSearch cmdlets
 July 1, 2020: You won't be able to use the New-MailboxSearch cmdlet to create new In-Place eDiscovery searches and In-Place Holds, but you can still use the other cmdlets to run, edit, and delete existing searches and holds at your own risk. Microsoft Support will no longer provide assistance for these types of searches and holds.
October 1, 2020: As previously stated, the In-Place eDiscovery Holds functionality in the EAC will be placed in a read-only mode. This also means that you won't be able to use the New-MailboxSearch, Start-MailboxSearch, or Set-MailboxSearch cmdlets. You'll only be able to get and remove existing searches and holds.
For more information, please see "https://docs.microsoft.com/en-us/microsoft-365/compliance/legacy-ediscovery-retirement?view=o365-worldwide" Retirement of legacy eDiscovery tools.

Type:

Tenant:

Effects for Operations	additions from MC200104: Automatic assignments via Exchange / PowerShell of legal hold might break.
Recommendations	additions from MC200104: Check your processes and tool, which set legal hold and eDiscovery functions and features, due to the retirement of Exchange Admin Center In-Place eDiscovery Holds, supporting cmdlets and EWS.
Links	MC200104
Description	additions from MC200104: Microsoft plans maasive changes to the eDiscovery and legal hold features.
Docu to check	Working instructions for IT Support, Service Description, Automation / Scripts
Linked Item Details	MC200104 Title : (Updated) Retirement of Exchange Admin Center In-Place eDiscovery and Holds MC200104 Url : https://docs.microsoft.com/microsoft-365/compliance/legacy-ediscovery-retirement MC200104 Info Url : https://docs.microsoft.com/microsoft-365/compliance/overview-ediscovery-20
More Info URL	https://docs.microsoft.com/microsoft-365/compliance/legacy-ediscovery-retirement
MS Preperations	Migrate all usage to Microsoft 365 eDiscovery or appropriate alternatives. These are described at: "https://docs.microsoft.com/en-us/microsoft-365/compliance/legacy-ediscovery-retirement" Retirement of legacy eDiscovery tools. If you're interested in migrating existing In-Place eDiscovery searches and holds to the Microsoft 365 compliance center, please see "https://docs.microsoft.com/en-us/microsoft-365/compliance/migrate-legacy-ediscovery-searches-and-holds?view=o365-worldwide" Migrate legacy eDiscovery searches and holds to the Microsoft 365 compliance center.
MS How does it affect me	Any holds created by using In-Place eDiscovery Holds in the EAC (or by using the corresponding cmdlet) will continue to preserve data. In-Place eDiscovery searches and holds can be removed at any time.

Reminder: Change in Process to Contact Microsoft Defender ATP Support

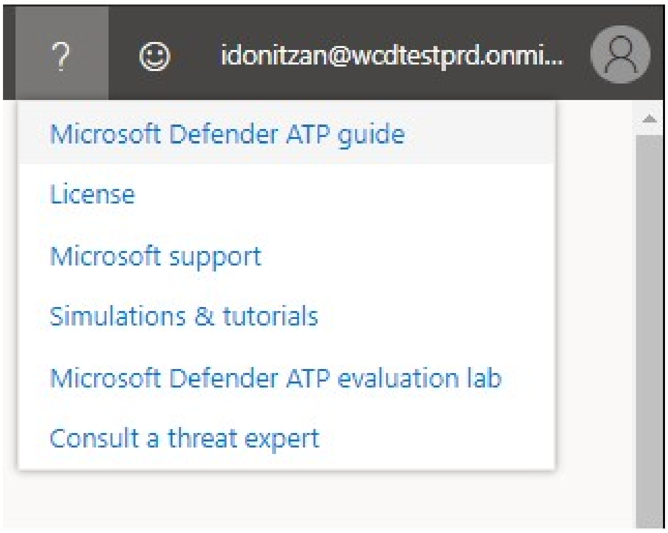
MC222822

check before: **10/01/2020**
Status:
Created: 09/25/2020
Product: Defender, Office app
Platform: World tenant, Online, Web
Scope: Administration, AI, Security
Ring:
Type: Admin impact
Tenant:

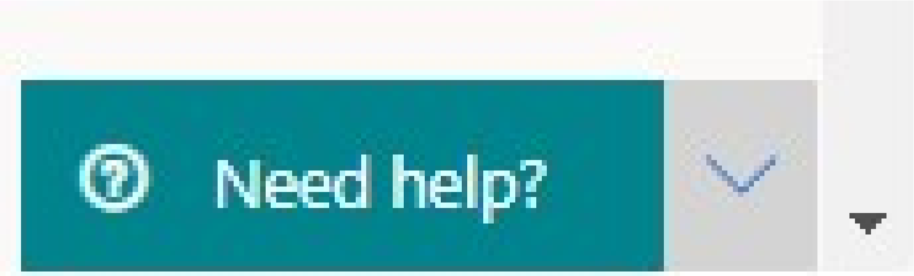
As originally announced in MC218778 (July '20) the process for opening support cases for Microsoft Defender ATP has changed with the availability of the new support widget. We completed rolling out the change in mid-September. Additionally, we wanted to provide additional guidance on which roles are needed to submit a Support request.

Links	MC218778
Pictures in MC	http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4C7AI?ver=7a1f http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4CcKo?ver=ec6a http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4C7AL?ver=ff03 http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4ChUH?ver=7379
Docu to check	Working instructions for IT Support, Service Description
Linked Item Details	MC218778 Title : Microsoft Defender ATP support case submission experience
MS Preperations	You may consider updating your training and documentation as appropriate. For more information on which roles have permission see, "https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#security-administrator-permissions" Security Administrator permissions. Roles that include the action "microsoft.office365.supportTickets/allEntities/allTasks" can submit a case. For general information on admin roles, see "https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide" About admin roles.
MS How does it affect me	Administrators can use this widget to: Find solutions to common problems Submit a support case to the Microsoft support team Note: At a minimum, one must have the Service Support Administrator OR Helpdesk Administrator role in order to open a case. Accessing the new support widget can be done in one of two ways: Clicking on the question mark on the top right of the portal and then clicking on “Microsoft support” Clicking on the “Need help?” button in the bottom right of the Microsoft Defender Security Center: In the widget you will be offered two options: Find solutions to common problems Open a service request Find solutions to common problems The “find solutions to common problems” option includes articles that might be related to the question you may ask. Just start typing the question in the search box and articles related to your search will be surfaced. In case the suggested articles are not sufficient, you can open a service request. Open a service request This option is available by clicking the icon that looks like a headset. You will then get the following page to submit your support case On this page, you fill in a title and description for the issue you are facing, as well as a phone number and email address where we may reach you. You may also include up to five attachments that are relevant to the issue in order to provide additional context for the support case. Finally, you select your time zone and an alternative language, if applicable. The request will be sent to Microsoft Support Team. We will respond to your service request shortly.

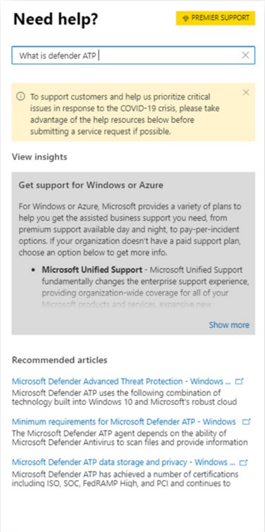
Image


?
idonitzan@wcdtestprd.onmi...
Microsoft Defender ATP guide
License
Microsoft support
Simulations & tutorials
Microsoft Defender ATP evaluation lab
Consult a threat expert

Image



Image



Need help?

What is defender ATP

To support customers and help us prioritize critical issues in response to the COVID-19 crisis, please take advantage of the help resources below before submitting a service request if possible.

View insights

Get support for Windows or Azure

For Windows or Azure, Microsoft provides a variety of plans to help you get the assisted business support you need, from premium support available day and night, to pay-per-incident options. If your organization doesn't have a paid support plan, choose an option below to get more info.

- **Microsoft Unified Support** - Microsoft Unified Support fundamentally changes the enterprise support experience, providing organization-wide coverage for all of your Microsoft products and services, expansive new

Show more

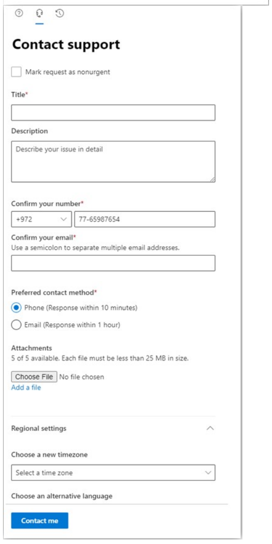
Recommended articles

Microsoft Defender Advanced Threat Protection - Windows ...
Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud

Minimum requirements for Microsoft Defender ATP - Windows
The Microsoft Defender ATP agent depends on the ability of Microsoft Defender Antivirus to scan files and provide information

Microsoft Defender ATP data storage and privacy - Windows ...
Microsoft Defender ATP has achieved a number of certifications including ISO, SOC, FedRAMP High, and PCI and continues to

Image



Contact support

☐ Mark request as nonurgent

Title*

Description
Describe your issue in detail

Confirm your number*
+972 77-65987654

Confirm your email*
Use a semicolon to separate multiple email addresses.

Preferred contact method*
● Phone (Response within 10 minutes)
○ Email (Response within 1 hour)

Attachments
5 of 5 available. Each file must be less than 25 MB in size.
Choose File No file chosen
Add a file

Regional settings

Choose a new timezone
Select a time zone

Choose an alternative language

Microsoft Information Protection: Data loss prevention for Microsoft Teams

65383

check before: **10/31/2020**

Data loss prevention (DLP) capabilities in Microsoft 365 government clouds will be extended to include Microsoft Teams chat and channel messages, including private channel messages. If your organization has DLP, you can now define policies that prevent people from sharing sensitive information in a Microsoft Teams channel or chat session.

Status: **In development**
Created: 06/27/2020
Product: Microsoft Information Protection, Teams
Platform: US Instances, World tenant, Online
Scope: Compliance, Security, Administration
Ring: General Availability
Type:
Tenant:

Docu to check Service Description, Working instructions for IT Support, User Knowledge base

More Info URL https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide

Microsoft Teams: Survivable Branch Appliance

68772

check before: **10/31/2020**

Survivable Branch Appliances (SBAs) are designed to ensure access to data and voice services in the event of a WAN outage. Microsoft is working with partners to provide this capability.

Status: **In development**
Created: 09/22/2020
Product: Teams
Platform: World tenant, Online
Scope: Administration, Security, Licensing
Ring: General Availability
Type: New feature, Admin impact
Tenant:

Docu to check Service Description, Working instructions for IT Support

What's next to do normal Items

Outlook mobile: S/MIME improvements and delegate permissions **MC220427**

check before:	**08/21/2020**
Status:	**varies**
Created:	08/15/2020
Product:	Intune, Office app, Outlook
Platform:	Android, iOS, mobile
Scope:	Administration, Security, User
Ring:	Monthly Channel (Standard)

For Outlook mobile clients, Microsoft is adding automatic signing and automatic message encryption using Secure Multipurpose Internet Mail extensions (S/MIME) as well as providing end user options to extend delegate mailbox permissions.
These updates are related to Microsoft 365 roadmap IDs "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=67271" 67271, "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=67272" 67272 (S/MIME) and "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=67273" 67273, "https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=67274" 67274 (delegate permissions).
When this will happen
Rollout for auto sign and auto encrypt with S/MIME will begin at the end of August and be complete by the end of September.
Rollout for delegate mailbox permissions for end users will begin in early September and be complete by the end of September.

Type:	Feature update, User impact	Tenant:

Links	67271,67272,67273,67274
Docu to check	User Knowledge base, Automation / Scripts, User Trainings
Linked Item Details	67271 Title : Outlook for iOS: Automatic signing and encryption 67271 Description: User setting to enable all messages to be automatically signed and encrypted using Secure Mobile Internet Mail extensions (S/MIME). 67272 Title : Outlook for Android: Automatic signing and encryption 67272 Description: User setting to enable all messages to be automatically signed and encrypted using Secure Mobile Internet Mail extensions (S/MIME). 67273 Title : Outlook for Android: End user options for Delegate permissions 67273 Description: You can extend permissions to have your delegate manage email and calendar events on your behalf by granting permission to read, create, change or delete items in your folders. Colleagues who have delegate permissions can add a Delegate Mailbox account to Outlook for Android. 67274 Title : Outlook for iOS: End user options to extend Delegate Permissions 67274 Description: You can extend permissions to have your delegate manage email and calendar events on your behalf by granting permission to read, create, change or delete items in your folders. Colleagues who have delegate permissions can add a Delegate Mailbox account to Outlook for iOS.
MS Preperations	The S/MIME user settings ship default Off. Administrators can use their mobile device management solution to require always sign and/or always encrypt with an app configuration policy on devices that are either enrolled or not enrolled. Microsoft Intune will include this option at the at the end of September. You might want to update user documentation and training.
MS How does it affect me	For organizations that use S/MIME for added security for email, this release allows users to set the S/MIME setting to “Always sign” and / or “Always encrypt”. After a user enables this setting, they will no longer have to manually set each email to be signed and encrypted. Valid S/MIME certificates are required to send signed and encrypted emails. Outlook mobile users can now grant delegate inbox permissions from within Outlook for iOS and Android. Users can set a delegate mailbox in order to allow others to take actions on their behalf. This release also adds the ability for users that have been granted folder level permissions from other Outlook endpoints to view those folders in Outlook mobile. These enhancements now complete our offering with shared and delegate mailbox scenarios. Organizations can enable access to another person’s mailbox using FullAccess permissions or users can grant others access to their mailboxes using Delegate permissions.

CAUTION New item - "Launched"

New Microsoft Stream: Unauthenticated external video sharing for videos in OneDrive and SharePoint

68829

check before: **08/31/2020**

Allow individual videos in OneDrive and SharePoint to be marked for unauthenticated external access allowing people to view the videos without a login by using the existing SharePoint file platform "Anyone" links. SharePoint admins can already control which users can make these kind of sharing links.

Status:	**Launched**
Created:	09/22/2020
Product:	OneDrive, SharePoint, Stream
Platform:	World tenant, Online
Scope:	Administration, User, Security, IT-Governance
Ring:	General Availability
Type:	New feature, User impact, Admin impact
Tenant:	

Docu to check User Trainings, User Knowledge base, Working instructions for IT Support

Office Apps: Security Update Report

68931

check before: **09/30/2020**

Keeping devices secure, compliant and up to date is a key to a environment secure. To help with that, you can access a new Security compliance report showing you the state of Office devices in your enterprise in relation to the uptake of the latest security patches available.

Status:	**In development**
Created:	09/25/2020
Product:	Office app
Platform:	World tenant, Online
Scope:	Security, Endpoint Management
Ring:	Preview
Type:	New feature, Admin impact
Tenant:	

Docu to check Working instructions for IT Support

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.

Reminder: Change in Process to Contact Microsoft Defender ATP Support

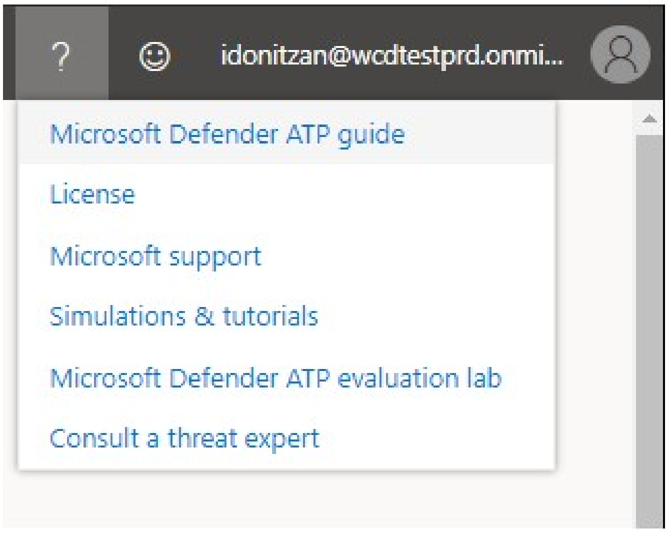
MC222827

As originally announced in MC218778 (July '20) the process for opening support cases for Microsoft Defender ATP has changed with the availability of the new support widget. We completed rolling out the change in mid-September. Additionally, we wanted to provide additional guidance on which roles are needed to submit a Support request.

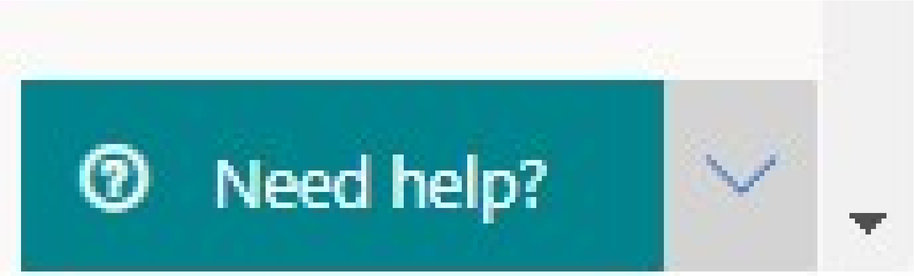
check before:	**10/01/2020**
Status:	
Created:	09/25/2020
Product:	Defender, Advanced Threat Protection - Azure (ATP), Advanced Threat Protection - Office 365, Azure Advanced Threat Protection
Platform:	World tenant, Online, Web
Scope:	Administration, AI, Security
Ring:	
Type:	Admin impact
Tenant:	

Links	MC218778
Pictures in MC	http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4C7AI?ver=7a1f http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4CcKo?ver=ec6a http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4C7AL?ver=ff03 http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4ChUH?ver=7379
Docu to check	Working instructions for IT Support, Service Description
Linked Item Details	MC218778 Title : Microsoft Defender ATP support case submission experience
MS Preperations	You may consider updating your training and documentation as appropriate. For more information on which roles have permission see, "https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#security-administrator-permissions" Security Administrator permissions. Roles that include the action "microsoft.office365.supportTickets/allEntities/allTasks" can submit a case. For general information on admin roles, see "https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide" About admin roles.
MS How does it affect me	Administrators can use this widget to: Find solutions to common problems Submit a support case to the Microsoft support team Note: At a minimum, one must have the Service Support Administrator OR Helpdesk Administrator role in order to open a case. Accessing the new support widget can be done in one of two ways: Clicking on the question mark on the top right of the portal and then clicking on “Microsoft support” Clicking on the “Need help?” button in the bottom right of the Microsoft Defender Security Center: In the widget you will be offered two options: Find solutions to common problems Open a service request Find solutions to common problems The “find solutions to common problems” option includes articles that might be related to the question you may ask. Just start typing the question in the search box and articles related to your search will be surfaced. In case the suggested articles are not sufficient, you can open a service request. Open a service request This option is available by clicking the icon that looks like a headset. You will then get the following page to submit your support case On this page, you fill in a title and description for the issue you are facing, as well as a phone number and email address where we may reach you. You may also include up to five attachments that are relevant to the issue in order to provide additional context for the support case. Finally, you select your time zone and an alternative language, if applicable. The request will be sent to Microsoft Support Team. We will respond to your service request shortly.

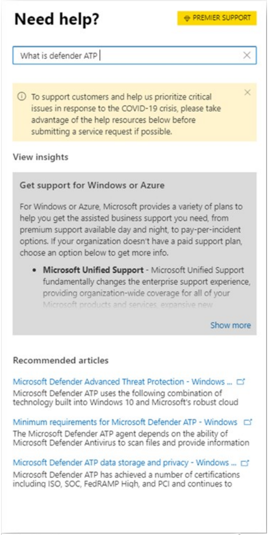
Image


?
idonitzan@wcdtestprd.onmi...
Microsoft Defender ATP guide
License
Microsoft support
Simulations & tutorials
Microsoft Defender ATP evaluation lab
Consult a threat expert

Image



Image



Need help?

What is defender ATP

To support customers and help us prioritize critical issues in response to the COVID-19 crisis, please take advantage of the help resources below before submitting a service request if possible.

View insights

Get support for Windows or Azure

For Windows or Azure, Microsoft provides a variety of plans to help you get the assisted business support you need, from premium support available day and night, to pay-per-incident options. If your organization doesn't have a paid support plan, choose an option below to get more info.

- **Microsoft Unified Support** - Microsoft Unified Support fundamentally changes the enterprise support experience, providing organization-wide coverage for all of your Microsoft products and services, expansive new

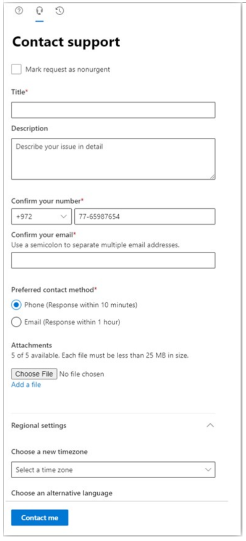
Recommended articles

Microsoft Defender Advanced Threat Protection - Windows ...
Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud

Minimum requirements for Microsoft Defender ATP - Windows
The Microsoft Defender ATP agent depends on the ability of Microsoft Defender Antivirus to scan files and provide information

Microsoft Defender ATP data storage and privacy - Windows ...
Microsoft Defender ATP has achieved a number of certifications including ISO, SOC, FedRAMP High, and PCI and continues to

Image



Contact support

☐ Mark request as nonurgent

Title*

Description
Describe your issue in detail

Confirm your number*
+972 77-65987654

Confirm your email*
Use a semicolon to separate multiple email addresses.

Preferred contact method*
● Phone (Response within 10 minutes)
○ Email (Response within 1 hour)

Attachments
5 of 5 available. Each file must be less than 25 MB in size.

No file chosen

Regional settings

Choose a new timezone
Select a time zone

Choose an alternative language

Microsoft Secure Score is removing one recommendation for Microsoft Defender ATP

MC222879

We’re updating Microsoft Secure Score improvement actions to ensure a more accurate representation of security posture.

check before:	**10/02/2020**
Status:	
Created:	09/26/2020
Product:	Defender
Platform:	World tenant, Online
Scope:	Administration, Security
Ring:	
Type:	Admin impact, Updated message
Tenant:	

Docu to check	Service Description, Working instructions for IT Support
MS Preperations	Based on customer feedback, we are removing the Set Microsoft Defender SmartScreen Windows Store app web content checking to warn security recommendation for Microsoft Defender ATP. "https://docs.microsoft.com/microsoft-365/security/mtp/microsoft-secure-score" Microsoft Secure Score is a measurement of an organization's security posture; it can be accessed at "https://security.microsoft.com/securescore" https://security.microsoft.com/securescore.
MS How does it affect me	We will begin rolling this out in mid-October; the rollout will be complete end of October.

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

MC222892

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.

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:	

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.

Windows Virtual Desktop: choose the EU geography to store the Windows Virtual Desktop service metadata

59889

Windows Virtual Desktop allows customers to pick the region best-suited to them to deploy their VMs. They should also get the choice of storing the service metadata in the geography best suited for their needs.

check before:	**10/31/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Windows Virtual Desktop
Platform:	World tenant, Online
Scope:	Administration, Compliance, Security
Ring:	Preview
Type:	Admin impact, New feature
Tenant:	

Docu to check	Automation / Scripts, Service Description

Microsoft 365 compliance center: Auto-apply retention labels for Teams meeting recordings

68689

With the storage of Teams meeting recordings moving to SharePoint and OneDrive, you can utilize the rich retention capabilities available in these platforms to manage the retention and deletion of meeting recordings. Support is also being added for automatic labeling capabilities to apply different retention periods or immutability to Teams meeting recording files, separated from the rest of your OneDrive and SharePoint files.

check before:	**10/31/2020**
Status:	**In development**
Created:	09/15/2020
Product:	Microsoft Compliance center, Teams
Platform:	World tenant, Online
Scope:	Compliance, Administration, Security
Ring:	Preview
Type:	Admin impact, New feature
Tenant:	

Docu to check Working instructions for IT Support, Service Description, Automation / Scripts

Outlook for Mac: iCloud account type support

68818

Adding support to add iCloud accounts within Outlook.

check before:	**10/31/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Outlook
Platform:	Mac, US Instances, World tenant
Scope:	Administration, Security, User
Ring:	Monthly Channel (Standard)
Type:	New feature, Admin impact
Tenant:	

Docu to check User Knowledge base

Office 365: Cross-Tenant People Search (Limited Availability)

67129

This feature is for customers with multiple tenants. It allows users to use People search to search across multiple tenants.

check before:	**11/30/2020**
Status:	**In development**
Created:	09/21/2020
Product:	Azure Active Directory, Exchange
Platform:	World tenant, Online
Scope:	User, Administration, Security, Compliance
Ring:	Preview, Limited Availability
Type:	Admin impact, New feature
Tenant:	

Docu to check Service Description, User Knowledge base

Microsoft Teams: Meeting recording improvements

68761

check before: **11/30/2020**

Stream playback performance and new features are coming to Teams meetings recordings by the end of the year as part of the new Stream experience. As part of this, meeting recordings will be stored in OneDrive, thus unlocking new value for customers including permissions and sharing, retention policies, basic information governance, increased quota, immediate meeting availability, "go local" tenant support, bring your own key (BYOK) support, multi-geo support, and improved transcript quality and speaker attribution.

Status: **In development**
Created: 09/22/2020
Product: OneDrive, Stream, Teams
Platform: World tenant, Online
Scope: Compliance, Multi-Geo, Administration, Security
Ring: General Availability
Type: New feature, Admin impact
Tenant:

Docu to check Service Description, User Knowledge base

SharePoint admin center - updated homepage dashboard

68812

check before: **11/30/2020**

When you first land in the SharePoint admin center, we want it to be both familiar and useful at a glance. The idea is to provide a familiar experience, taking a similar design approach as the Microsoft admin center. You’ll see more and more cards and graphs appear over time – so you can see insights on files, usage security, recommendations, training and so on. Better see what’s happening, and then take the appropriate action.

Status: **In development**
Created: 09/22/2020
Product: Microsoft 365 admin center, SharePoint
Platform: US Instances, World tenant, Online, Web
Scope: Administration, Security
Ring: Targeted Release
Type: Feature update, Admin impact
Tenant:

Docu to check Working instructions for IT Support

Outlook for Mac: S/MIME

68817

check before: **11/30/2020**

Status: **In development**

Created: 09/22/2020

Product: Outlook

Platform: Mac, US Instances, World tenant

Scope: UI, Security, Administration

Ring: Monthly Channel (Standard)

Type: New feature, Admin impact, User impact

Tenant:

Support for S/MIME - S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted method (or more precisely, a protocol) for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them.

Docu to check Service Description, User Knowledge base, Working instructions for IT Support

What's next to do minor Items

Advanced Audit: User searches

68806

check before: **08/31/2020**

Status: **Rolling out**

Created: 09/22/2020

Product: Exchange, Microsoft Compliance center

Platform: Online, World tenant

Scope: Compliance, Security

Ring: General Availability

Type: New feature

Tenant:

User search event, which is generated when a user search was performed on Exchange Online or SharePoint Online. This is valuable especially if a malicious actor accessed an account to search for sensitive material. By analyzing the search query, an investigator can understand the kind of content being searched for.

Docu to check Working instructions for IT Support

Microsoft Teams: Graph API permissions

68759

check before: **08/31/2020**

Status: **Rolling out**

Created: 09/22/2020

Product: Graph API, Teams

Platform: Developer, World tenant

Scope: Administration, Developer, Security

Ring: General Availability

Type: New feature, Admin impact

Tenant:

Administrators will be able to grant consent to Graph API permissions, on behalf of the entire tenant, they will be able to see granular permissions and provide resource-specific consent, simplifying app management procedure all in one place.

Docu to check Working instructions for IT Support, Automation / Scripts

---

CAUTION New item - "Launched"

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

70742

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:

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

Docu to check Working instructions for IT Support

Advanced Audit: Mail send events

68807

check before: **08/31/2020**

Status: **Rolling out**

Created: 09/22/2020

Product: Exchange, Microsoft Compliance center, Yammer, OneDrive

Platform: World tenant, Online

Scope: Compliance, Security

Ring: General Availability

Type: New feature

Tenant:

Mail send event is generated when a user sends, replies to, or forwards an email. Whether the action was malicious or unintentional, this event can let investigators know what metadata was contained in the emails sent from a compromised account.

Docu to check Working instructions for IT Support

Advanced eDiscovery now supports linked content (modern attachments) from OneDrive and SharePoint Online

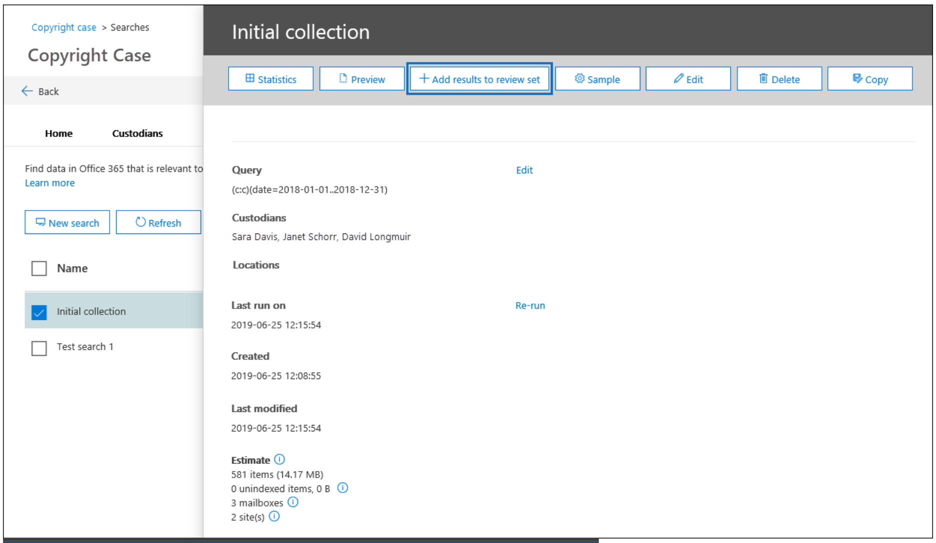
MC222627

check before:	**09/29/2020**
Status:	**Rolling out**
Created:	09/23/2020
Product:	eDiscovery, Exchange, Office 365 Advanced Compliance, OneDrive, Outlook, SharePoint, Teams, Yammer
Platform:	Online, Web, World tenant
Scope:	Administration, Compliance, Security, User
Ring:	General Availability
Type:	Admin impact, New feature
Tenant:	

Advanced eDiscovery will now support linked content (modern attachments) from OneDrive and SharePoint Online (OD/SPO). Linked content can be shared in Teams and Yammer chat messages and Outlook emails.
This message is associated with Microsoft 365"https://www.microsoft.com/microsoft-365/roadmap?filters=searchterms=66185" Roadmap ID 66185.
When this will happenWe will begin rolling this out in late September and expect the rollout to be complete by the end of October.

Links	66185
Pictures in MC	https://docs.microsoft.com/microsoft-365/media/c1b4fc00-7a15-4587-b9b0-ce594bb02e4d.png http://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4GbHJ?ver=4c5bf
Docu to check	Working instructions for IT Support
Linked Item Details	66185 Title : Advanced eDiscovery: Supporting linked content from OneDrive and SharePoint Online (modern attachments) 66185 Description: To help streamline discovery of linked content, Advanced eDiscovery natively groups linked content from OneDrive and SharePoint Online in the same family as the original Outlook email or Teams and Yammer chat message—streamlining the process of collecting, reviewing, and exporting the related content without additional configuration.
MS Preperations	Ask the Advanced eDiscovery manager in your organization to review this new functionality in a pre-production tenant and to determine how your organization might use this enhanced document retrieval in its investigations. Learn more: "https://docs.microsoft.com/microsoft-365/compliance/add-data-to-review-set#define-options-to-scope-your-collection-for-review" Define options to scope your collection for review "https://techcommunity.microsoft.com/t5/microsoft-security-and/improving-ediscovery-workflows-and-enhancing-your-forensic/ba-p/1696658" Improving eDiscovery workflows and enhancing your forensic investigations
MS How does it affect me	Advanced eDiscovery in Microsoft 365 provides an end-to-end workflow to preserve, collect, review, analyze, and export data that's responsive to your organization's internal and external investigations. When Advanced eDiscovery administrators and managers use the Search tool to identify relevant documents, they can add those search results to a review set. Exchange 2016 introduced document collaboration that allowed on-premises users to integrate attachments stored on OD/SPO directly into email sent from Outlook on the web. Document collaboration is now supported by all Outlook clients. Rather than attach a file to an email, users insert a link to a file that is stored in OD/SPO. This feature is often called modern attachments, and it reduces storage demands on the Exchange server. However, because these files are stored outside of the Exchange server, until now they were not included in a collection and review set. Your Advanced eDiscovery team now has three options for collecting the results of a search into a review set (pre-existing or new): Conversational review set (beta) Select this to see email and chat enabled as threaded conversations. Enable retrieval for modern attachment Select this to review documents referenced in Outlook as a modern attachment (a link to a SPO/ODB source) as well as any SPO/ODB documents that are included as a link in Outlook or Teams. Include versions from SharePointSelect this to make a copy of all versions of a SharePoint file per the version limits and search parameters of the collection.

Image



Find data in Office 365 that is relevant to

Initial collection

Query
(c:c)(date=2018-01-01..2018-12-31)

Custodians
Sara Davis, Janet Schorr, David Longmuir

Locations

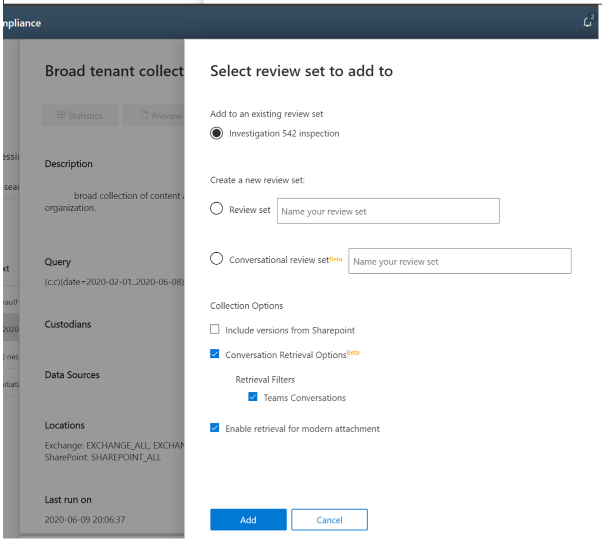
Last run on
2019-06-25 12:15:54

Created
2019-06-25 12:08:55

Last modified
2019-06-25 12:15:54

Estimate
581 items (14.17 MB)
0 unindexed items, 0 B
3 mailboxes
2 site(s)

Image



Description
broad collection of content
organization.

Query
(c:c)(date=2020-02-01..2020-06-08)

Custodians

Data Sources

Locations
Exchange: EXCHANGE_ALL, EXCHAN
SharePoint: SHAREPOINT_ALL

Last run on
2020-06-09 20:06:37

Select review set to add to

Add to an existing review set
● Investigation 542 inspection

Create a new review set:
○ Review set Name your review set

○ Conversational review set^Beta Name your review set

Collection Options
☐ Include versions from Sharepoint
☑ Conversation Retrieval Options^Beta
Retrieval Filters
☑ Teams Conversations
☑ Enable retrieval for modern attachment

Intune: New Endpoint Security Antivirus reports

MC222596

check before:	**09/29/2020**
Status:	
Created:	09/22/2020
Product:	Defender, Intune, Microsoft 365 admin center
Platform:	World tenant, Online
Scope:	Administration, MDM, Security
Ring:	
Type:	
Tenant:	

We are introducing new Microsoft Defender Antivirus reports in the Microsoft Endpoint Manager admin center to help you monitor your devices for status on malware and antivirus states. You will be able to use two new operational reports to see which devices need your attention and two organizational reports to view general antivirus information.

Docu to check	Working instructions for IT Support
More Info URL	https://aka.ms/new-endpoint-security-av-reports
MS Preperations	Familiarize yourself with the new reports and update your documentation if needed. For more information on reporting, see "https://docs.microsoft.com/mem/intune/fundamentals/reports" Intune reports and "https://docs.microsoft.com/mem/intune/protect/endpoint-security" Manage endpoint security in Microsoft Intune.
MS How does it affect me	We're adding four new reports for Microsoft Defender Antivirus on Windows 10 in Microsoft Endpoint Manager. These reports include: Two operational reports, Windows 10 unhealthy endpoints and Windows 10 detected malware. In Microsoft Endpoint Manager, select Endpoint security > Antivirus. Two organizational reports, Antivirus agent status and Detected malware. In Microsoft Endpoint Manager, select Reports > Microsoft Defender Antivirus. We encourage you to use these new reports over the legacy Threat Agent Status report which we will be deprecating in the future. Learn more about these reports on the blog: "https://aka.ms/new-endpoint-security-av-reports" https://aka.ms/new-endpoint-security-av-reports

---

Microsoft Information Protection: Auto-classification with sensitivity labels in SPO, EXO, OneDrive for gov clouds

67125

Auto-classification with sensitivity labels in OneDrive, SharePoint Online, and Exchange Online will soon be available in GCC and GCC-High environments. Sensitivity labels are central to Microsoft Information Protection, enabling you to label important content to associate it with protection policies and actions like encryption and visual marking. With this release, you can start using sensitivity labels at scale for documents stored on OneDrive and SharePoint Online, and for emails in transit in Exchange Online automatically without manual user input.

check before:	**09/30/2020**
Status:	**In development**
Created:	09/16/2020
Product:	Exchange, Information Protection - Office 365, Microsoft Information Protection, OneDrive, SharePoint
Platform:	Online, US Instances
Scope:	Compliance, Security, User
Ring:	General Availability
Type:	New feature, Admin impact
Tenant:	

Docu to check	Service Description, Automation / Scripts, User Knowledge base
More Info URL	https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange

Microsoft Teams: Microsoft Teams EHR connector

68728

The new Microsoft Teams EHR connector will allow clinicians and patients to launch a virtual patient visit or consult with another provider in Teams directly from their electronic health record system.

check before:	**09/30/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Teams
Platform:	World tenant, Online
Scope:	Compliance, Security, Administration
Ring:	General Availability
Type:	New feature
Tenant:	

Docu to check Service Description, User Knowledge base

Records Management: Regulatory record labels

MC222757

As announced at Ignite, we're introducing the public preview of regulatory record labels which further enhance immutability of labeled items. These new labels prevent metadata changes, records movements, and records versioning. They also block users and administrators from removing a label once applied.

This message is associated with Microsoft 365 "https://www.microsoft.com/microsoft-365/roadmap?filters=&searchterms=63062" Roadmap ID 63062.

When this will happenThis feature is available now worldwide.

check before:	**10/01/2020**
Status:	**Rolling out**
Created:	09/24/2020
Product:	Exchange, OneDrive, SharePoint, Skype for Business, Teams
Platform:	Online, World tenant
Scope:	Administration, Compliance, Security
Ring:	Preview, Targeted Release
Type:	Admin impact, New feature
Tenant:	

Links	63062
Docu to check	Service Description, User Knowledge base, Working instructions for IT Support
Linked Item Details	63062 Title : Records Management: Regulatory Records (public preview) 63062 Description: Provides customers the ability to declare items in SharePoint Online as regulatory items. These labels are more stringent label vs record labels. Targeted to Financial services or other industries who have WORM compliance requirements. Will update the Cohasset assessment to include SharePoint Online. 63062 Url : https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide
MS Preperations	Review a "https://docs.microsoft.com/microsoft-365/compliance/records-management#compare-restrictions-for-what-actions-are-allowed-or-blocked" detailed comparison of the restrictions a regulatory record label enforces, including which actions are allowed or blocked. If you would like to take advantage of this new functionality, "https://docs.microsoft.com/microsoft-365/compliance/declare-records" here's how to get started. "https://docs.microsoft.com/microsoft-365/compliance/records-management" Learn about records management in Microsoft 365.
MS How does it affect me	If your organization requires records to comply with high immutability standards, you can leverage regulatory record labels to enforce the maximum restrictions available in Microsoft 365. This new capability, when configured as recommended, can help you meet SEC 17a-4, FINRA Rule 4511, and CFTC Rule 1.31 (c) – (d) requirements for SharePoint, OneDrive for Business, Exchange email messages, and certain Teams and Skype for Business content.

Information Governance: Retention for Yammer messages

MC222893

As announced at Ignite, we’re "https://techcommunity.microsoft.com/t5/microsoft-security-and/what-s-new-in-microsoft-information-governance-and-records/ba-p/1681207" introducing the public preview of retention policies for Yammer for user and community messages in Yammer.

This message is associated with Microsoft 365 "https://www.microsoft.com/microsoft-365/roadmap?rtc=1&filters=&searchterms=63064" Roadmap ID 63064.

When this will happenWe’ll begin gradually rolling this out at the beginning of October and expect it to be complete by early November.

check before:	**10/03/2020**
Status:	**In development**
Created:	09/26/2020
Product:	Microsoft Compliance center, Yammer
Platform:	World tenant, Online
Scope:	Administration, Compliance, Security
Ring:	Preview
Type:	Admin impact, Feature update
Tenant:	

Links	63064
Docu to check	User Knowledge base, Working instructions for IT Support
Linked Item Details	63064 Title : Information Governance: Retention policies for Yammer 63064 Description: Expand support for Yammer messages. 63064 Url : https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-information-governance?view=o365-worldwide
MS Preperations	To leverage retention policies for Yammer messages, make sure that your Yammer Enterprise network is in "https://docs.microsoft.com/yammer/configure-your-yammer-network/overview-native-mode" Native Mode. Once your Yammer network is in Native Mode, go "https://compliance.microsoft.com/" Microsoft 365 compliance center and use the Information Governance solution to create a new retention policy for Yammer messages.
MS How does it affect me	If you are using Yammer Enterprise within your organization and wish to set retention or deletion policies to ensure you’re keeping only the data you need in your tenant, you will be able to "https://docs.microsoft.com/microsoft-365/compliance/create-retention-policies#retention-policy-for-yammer-locations" target Yammer communities and users with new or existing retention policies.

Windows Virtual Desktop: Migration tool for non-ARM to ARM objects

63945

Objects created with the Windows Virtual Desktop classic) GA release are non-ARM and cannot be managed by the Azure portal without explicit migration to the ARM model. A tool will be provided by Microsoft that will allow customers to migrate their non-ARM Windows Virtual Desktop objects to ARM Windows Virtual Desktop objects in a simplistic manner.

check before:	**10/31/2020**
Status:	**In development**
Created:	09/17/2020
Product:	Windows Virtual Desktop
Platform:	Windows Desktop, World tenant
Scope:	Administration, MDM, Security
Ring:	Preview
Type:	Feature update, Admin impact
Tenant:	

Docu to check	Automation / Scripts, Working instructions for IT Support

Outlook for Mac: IMAP account type support

68819

Adding support to add IMAP accounts within Outlook.

check before:	**11/30/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Outlook
Platform:	Mac, US Instances, World tenant
Scope:	Administration, Security, User
Ring:	Monthly Channel (Standard)
Type:	New feature, Admin impact, User impact
Tenant:	

Docu to check User Trainings, User Knowledge base

Windows Virtual Desktop: protection from screen scraping

70197

With this feature enabled, administrator can prevent users from accidentally sharing the protected content.

check before:	**11/30/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Windows Virtual Desktop
Platform:	World tenant, Online
Scope:	Administration, Security
Ring:	Preview
Type:	New feature
Tenant:	

Docu to check Working instructions for IT Support, Automation / Scripts

---

Microsoft Teams: Access files offline on mobile

68750

The Teams mobile app now allows you to access files even when you are offline or in bad network conditions. Simply select the files you need access to, and Teams will keep a downloaded version to use in your mobile app. You will find all your files that are available offline in the files section of the app.

check before:	**11/30/2020**
Status:	**In development**
Created:	09/22/2020
Product:	Teams
Platform:	mobile, World tenant
Scope:	User, Security
Ring:	General Availability
Type:	New feature
Tenant:	

Docu to check User Knowledge base

SharePoint admin center - Migration Manager: Box migrations (public preview) 68816

check before: **11/30/2020**

With our recent Mover acquisition, we are excited to expand our capabilities to allow moving content from third-party cloud storage providers starting with Box.com. When you’re ready to move your content, click on the Migrate tab in the SharePoint admin center to start scan discovery, assessment, and migrate. You'll get detailed reports and the rest in a seamless transition of files and folders to Microsoft 365.

Status: **In development**
Created: 09/22/2020
Product: Microsoft 365 admin center, SharePoint
Platform: US Instances, World tenant, Online
Scope: Administration, Security, Compliance
Ring: Targeted Release
Type: New feature, Admin impact
Tenant:

Docu to check Automation / Scripts, Service Description

Microsoft Information Protection: UI for configuring Exact Data Match 67100

check before: **11/30/2020**

Admins will be able to configure and edit Exact Data Match (EDM) from within the Microsoft 365 Compliance Center, providing an alternative to configuring EDM from PowerShell.

Status: **In development**
Created: 08/14/2020
Product: Microsoft Compliance center, Microsoft Information Protection
Platform: Web, Online, World tenant
Scope: Administration, Compliance, Security
Ring: Preview
Type: Admin impact
Tenant:

Docu to check Working instructions for IT Support

Microsoft Teams: By invitation only meetings 68730

check before: **11/30/2020**

Organizers will be able to schedule invite-only meetings where only authorized participants will be allowed to join.

Status: **In development**
Created: 09/22/2020
Product: Teams
Platform: World tenant, Online
Scope: Security, User
Ring: General Availability
Type: New feature, User impact
Tenant:

Docu to check User Knowledge base

Microsoft Teams: Meeting Recap

68729

check before: **11/30/2020**

Meeting recap will help teams stay on track and keep their work moving forward after the meeting is over. Coming this year, a recap with the meeting recording, transcript, chat, shared files and more will be shared with participants in the meeting Chat tab and viewable in the Details tab for each meeting.

Status: **In development**
Created: 09/22/2020
Product: Teams
Platform: World tenant, Online
Scope: Security, Compliance, User
Ring: General Availability
Type: New feature
Tenant:

Docu to check User Knowledge base

Yammer: Browse community files stored in SharePoint with SharePoint library structure and capabilities.

67240

check before: **11/30/2020**

Browsing files that have been uploaded to a Yammer community will now have access to the SharePoint files structure and capabilities.

Status: **In development**
Created: 09/16/2020
Product: SharePoint, Yammer
Platform: World tenant, Online, Web
Scope: User, Security
Ring: General Availability
Type: Feature update, User impact
Tenant:

Docu to check User Knowledge base

Microsoft Teams: Customer Key support (Preview)

68732

check before: **11/30/2020**

Microsoft helps keep Teams data safe by encrypting it while at rest in Microsoft datacenters. Now we are extending this capability to enable customers to add a layer of encryption using their own keys for Teams, similar to Exchange Online, SharePoint Online and OneDrive.

Status: **In development**
Created: 09/22/2020
Product: Teams
Platform: Online, World tenant
Scope: Security, Compliance, Administration
Ring: Preview
Type: New feature, Admin impact
Tenant: