cloudscout.one what's next CW 39

Product: Defender

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.

What's next to do Major Items

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.

Reminder: Change in Process to Contact Microsoft Defender ATP Support

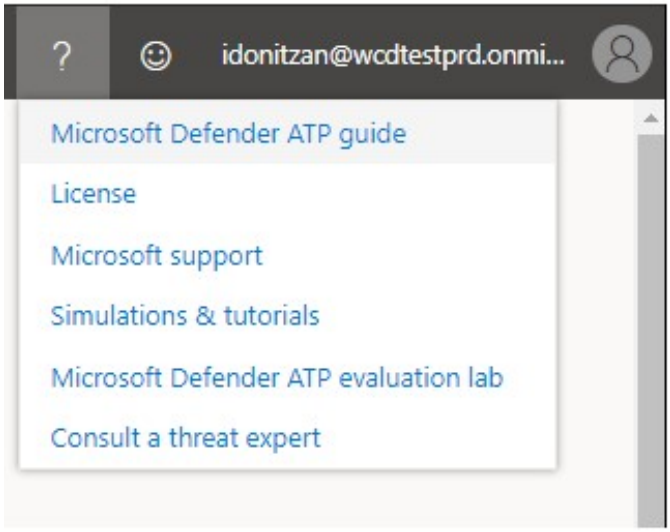
MC222822

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.

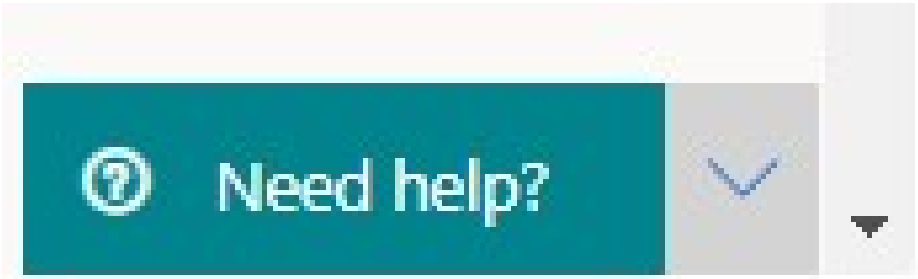
		check before:	**10/01/2020**
		Status:	
		Created:	09/25/2020
		Product:	Defender, Office app
		Platform:	World tenant, Online, Web
		Scope:	Administration, AI, Security
		Ring:	
	Type:	Admin impact	Tenant:

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.

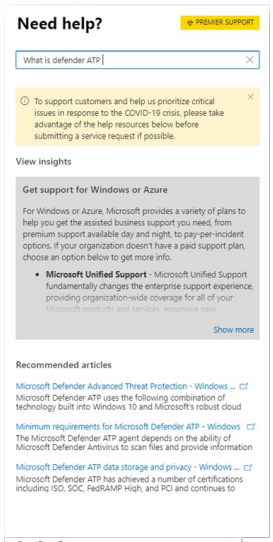
Image



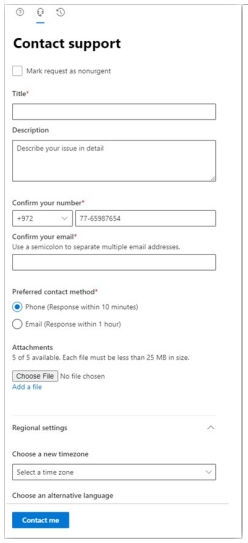
Image



Image



Image



What's next to do normal Items

Reminder: Change in Process to Contact Microsoft Defender ATP Support

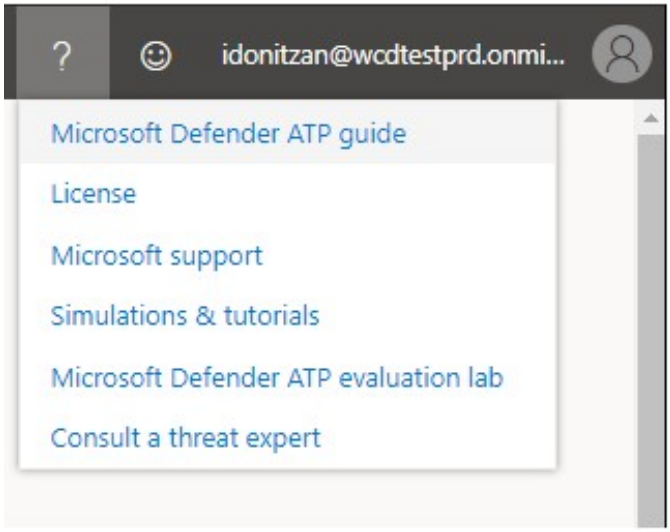
MC222827

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.

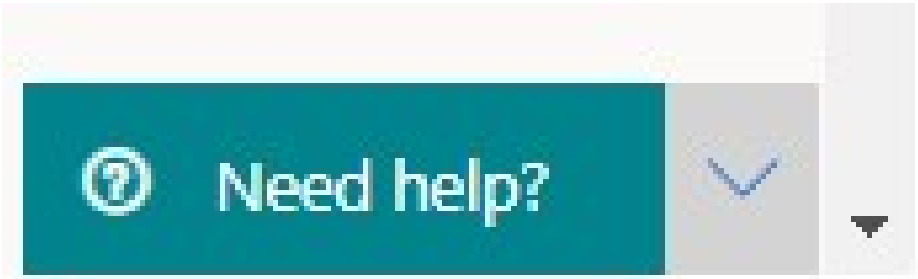
check before:	**10/01/2020**
Status:	
Created:	09/25/2020
Product:	Defender, Advanced Threat Protection - Azure (ATP), Advanced Threat Protection - Office 365, Azure Advanced Threat Protection
Platform:	World tenant, Online, Web
Scope:	Administration, AI, Security
Ring:	
Type: Admin impact	Tenant:

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.

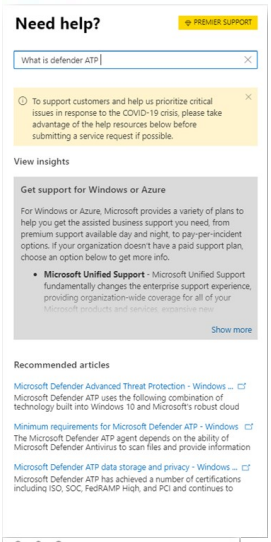
Image



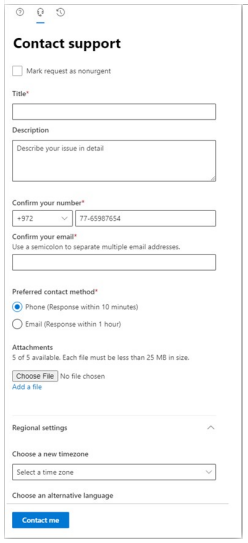
Image



Image



Image



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.

What's next to do minor Items

Intune: New Endpoint Security Antivirus reports

MC222596

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.

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:

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

---