



Webinar FAQ:

Microsoft On-Premises DLP

Prepared by:

Microsoft 365 Security & Compliance Team, November 2020

- **Sign up** for the MIPC Preview Program: <https://aka.ms/MIPC/JoinPreviews>
- **Follow** us on twitter: twitter.com/MIPnews
- **View** the On-Premises DLP documentation for additional information:
 - <https://techcommunity.microsoft.com/t5/microsoft-security-and/find-your-unscanned-and-overexposed-shares-on-premises-with-an/ba-p/1744783>
 - <https://techcommunity.microsoft.com/t5/microsoft-security-and/migrating-from-exchange-transport-rules-to-unified-dlp-the/ba-p/1749723>
 - <https://docs.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/data-loss-prevention>
 - <https://techcommunity.microsoft.com/t5/microsoft-security-and/microsoft-endpoint-dlp-webinar/ba-p/1799875>
- **Submit** through UserVoice for Records management and share your feature asks here to help us prioritize and shape the solution:
<https://office365.uservoice.com/forums/289138-office-365-security-compliance/category/379531-information-governance-and-records-management>
- **Watch** previous webinars: <http://aka.ms/MIPC/webinars>

Features & Updates

Q: Is this supposed to replace on premise AIP File Scanner? If not, what would the integration entail?

A: It is an additional capability that is DLP focused and based on AIP Scanner infrastructure.

Q: Is this integrated with the AIP client add-in, and/or is it included Office apps?

A: It's part of AIP Scanner from infrastructure deployment side, and included in AIP client package. It is not included in Office Apps.

Q: Just Windows File share or are others included?

A: This is an additional feature of the existing AIP Scanner - so anything we can reach over SMB protocol. This can be a NAS, SAN, or anything else as long as we can talk to it over SMB, or SharePoint Server 2013/2016/2019

Q: What license is required for on-prem DLP?

A: We require M365 E5 / E5 Compliance / AIP P2/ EMS E5 / IPG as part of the preview program but it's not a final commitment for GA. License requirements will be published in our MS Docs: <https://aka.ms/MIPC/Licensing> (there is a PDF file and XLS file on that page that goes into details).

Q: Is this information (DLP on-premises preview) public?

A: The feature is in private preview. The public information is this webinar which will be posted at aka.ms/mipc/webinars

Q: What is the capacity per one scanner? How to scale AIP scanner infrastructure?

A: You can check out our MS docs on optimization for Scanner - <https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-configure-install-classic#optimizing-scanner-performance>.

Q: Which licenses are needed for Activity Explorer and Content Explorer?

A: We detail these in our MS Docs - <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide>.

Q: Does the customer need two valid licenses: endpoint DLP and office 365 E3 for all DLP capabilities data on email, rest and motion?

A: IP&G and Office 365 E3.

Q: Does DLP cover Skype and Teams?

A: Teams chat and channel messages. Skype needs to be in Hybrid mode.

Q: Can we have multiple DLP policies for different groups?

A: Depends on the workload you are configuring for DLP. EXO = Distribution Groups, SPO = Per Site, OD4B = Per Site, Teams = Per Team, Devices = Per User/Group, MCAS = per MCAS instance and Scanner = Per File Path. You can have as many policies targeting these same targets as you like.

Q: Can DLP cover AWS?

A: Via MCAS, yes.

Q: Can DLP cover SVN?

A: Not natively. If the SVN client is installed on a machine, it can be configured as an unallowed app to block transfers.

Q: Can DLP be integrated with our Helpdesk tool?

A: DLP events can be exported via the O365 Management API. If your helpdesk tool can integrate with this, then yes.

Q: Any plan to extend AIP Scanner to on-premises mailboxes?

A: It's in our backlog, but less prioritized than other features, so it's not planned to be added in next 9 months.

Q: Will this include parameters from the header of the file? If there is a secret in the header and I want this to be matched with a DLP policy for on-prem files?

A: Yes, file headers are inspected when we match the DLP condition for sensitive info types.

Q: If one quarantine is done, could we receive one email/notification and release the quarantine if false positive?

A: Not now. We are looking into providing an option for admins / file owners to get notifications on quarantine events and allow them to act upon them.

Q: How do we define an on-prem file share document as public - which groups need to be present on the ACL, authenticated users etc.? Can we define groups that if present on the ACL, will call that document as public?

A: We consider the share, folder, or file as publicly accessible if one of the following entities are granted direct permissions on the object:

- Everyone
- NT Authority\Authenticated Users
- Domain\Domain Users

If one of these groups are added to another group that is granted access to the object this will not be detected.

Q: You demonstrated the capability between 3 portals: Azure, M365 Compliance and SCC for audit logs. Will you consolidate it under one portal at some point?

A: *It's one of the most common asks. We work on bringing all into one portal (M365 Compliance). For DLP work you will mostly need M365 portal only expect of few operational tasks.*

Q: Any plans to have AIP/MIP and DLP completely joint under one name and configured from one section?

A: *Thank you for this feedback, we are looking into this as part of the future roadmap.*

Q: When is GA planned?

A: *It is too late to commit to GA dates, but if everything goes as expected we plan to open this to public preview in January and GA this later in Q2 CY2021. This mainly depends on number of customers that preview this in private preview and provide their feedback to increase confidence on what we ship. Therefore, your feedback is needed at this stage.*

Q: Is there any possible way to set DLP policies to specific accounts regarding SharePoint and OneDrive?

A: *We are working to improve the OneDrive scoping in the future. SharePoint scoping is site related as it makes more sense due to the product design.*

Q: Any way to get a GCC (not GCC High) customer in the preview?

A: *Currently neither GCC nor GCC High tenants can be onboarded to the preview. We recommend creating a new trial tenant in commercial cloud to preview this. Based on the demand from GCC and GCC-High customers we will prioritize these environments for public preview availability.*

Q: Any ability to enforce other restrictions during scan, like second factor (e.g. additional password/secret) to be able to access AIP labeled data as highly confidential?

A: *Enforcing MFA for accessing content sound more like a DLP for data in use which is not done by scanner. There are more actions that we plan to bring to scanner post GA and we are looking for customer feedback on what would you like us to add. Feel free to contact us offline and share your thoughts.*

Q: Any potential ETA for "public" preview?

A: *Currently planned for January, but it depends on the number of customers participating in private preview and level of confidence we can get from the private preview.*

Q: Regarding licenses for activity and content explorer, it says Microsoft 365 (E5/A5) Office 365 (E5), Advanced Compliance (E5) add-on, Advanced Threat Intelligence (E5) add-on. Does this mean customers with AIP (EMS E3 or E5 don't have access to it?

A: *For this preview you can add one trail M365 E5/Compliance E5 license to use Activity Explorer. For prod deployment current licensing requires M365 E5/Compliance E5. Existing AIP customer that use AIP analytics will be contacted on this matter once the licensing for migrating customers is closed.*

Q: When will the AIP log analytics workspace capabilities be moved over to the M365 Compliance portal and will we still be able to programmatically extract the analytics as we do with ALA today?

A: You can access raw logs in O365 Audit using an API [Office 365 Management Activity API reference | Microsoft Docs](#)