



Microsoft Defender Advanced Threat Protection Tutorial

Threat & Vulnerability Management

May 2019

*Microsoft confidential
(Preview)*

Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2019 Microsoft. All rights reserved.

Please refer to [Microsoft Trademarks](#) for a list of trademarked products.

All other trademarks are property of their respective owners.

Introduction

This do-it-yourself guide will walk you through some of the basic scenarios that our next generation Threat & Vulnerability Management capability, built into Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP), has to offer.

We will explore how this new capability uses a game-changing risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.

As a component of Microsoft Defender ATP's unified endpoint security platform that is integrated to multiple services in Microsoft Threat Protection, this new Threat & Vulnerability Management capability also provides Security Administrators with the following unique values:

- Real-time endpoint detection and response (EDR) insights correlated with endpoint vulnerabilities
- Invaluable machine vulnerability context during incident investigations
- Built-in remediation ticketing processes through Microsoft Intune and Microsoft System Center Configuration Manager (SCCM)

Effectively identifying, assessing, and remediating endpoint weaknesses is pivotal in running a healthy security program and reducing organizational risk. Threat & Vulnerability Management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience. It bridges the gap among security stakeholders: Security Administrators, Security Operation personnel, and IT Administrators.

Scenario 1 will show you how to reduce your organization's threat and vulnerability exposure.

Scenario 2 will take you through the tie that binds vulnerability monitoring and remediation workflows.

Scenario 3 will explain when you can file for recommendation exceptions and how you can handle them

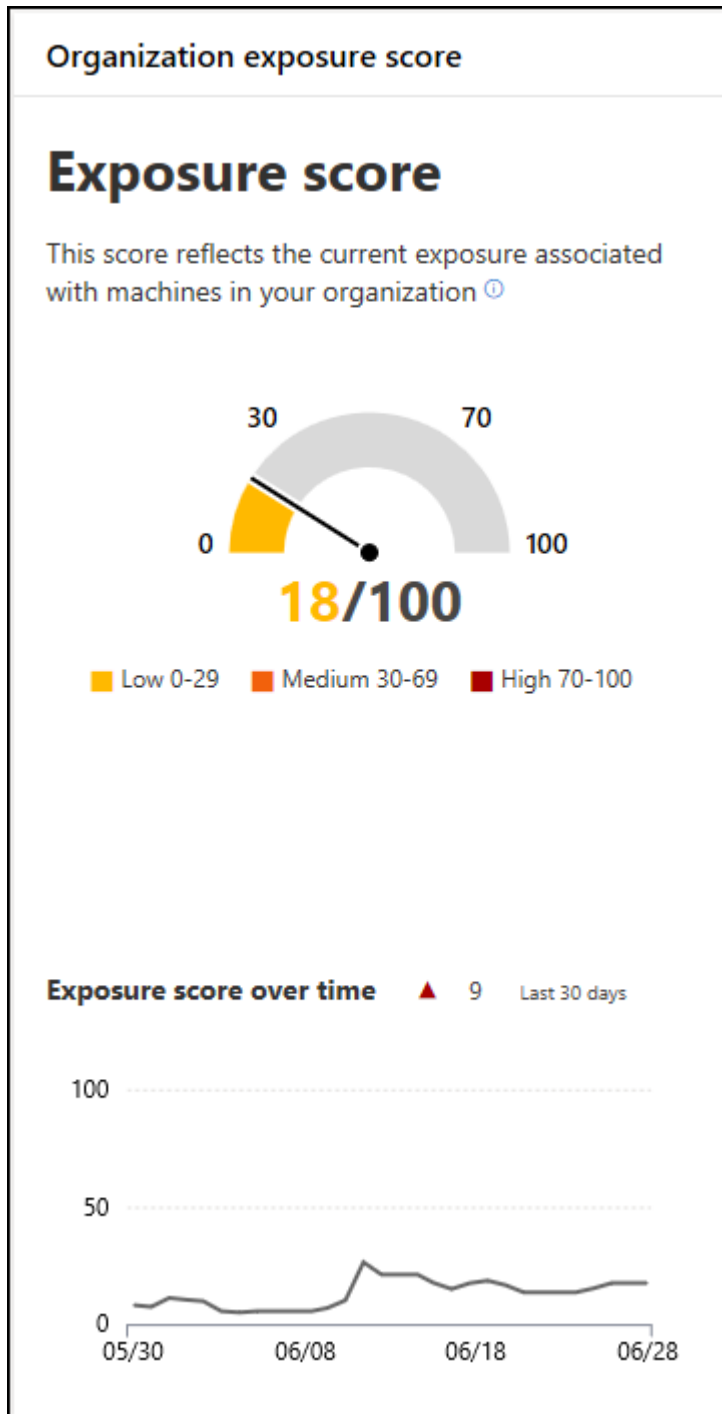
The test machine required for the simulations should:

- Be onboarded to Microsoft Defender ATP
- Run Windows 10 1709 (Fall Creators Update) or later
- Have at least one security recommendation that can be viewed in the machine page

For onboarding instructions, [read to the product guide](#). We recommend running the local onboarding script to onboard the test machine.

Scenario 1: Exposure level improvement

Microsoft Defender ATP's Threat & Vulnerability Management introduces a new exposure score metric which visually represents how exposed your machines are to imminent threats.



The exposure score is continuously calculated on each device in the organization and influenced by the following factors:

- Weaknesses, such as vulnerabilities and misconfigurations discovered on the device
- External and internal threats such as public exploit code and security alerts
- Likelihood of the device getting breached given its current security posture
- Value of the device to the organization given its role and content

The exposure score is broken down into the following levels:

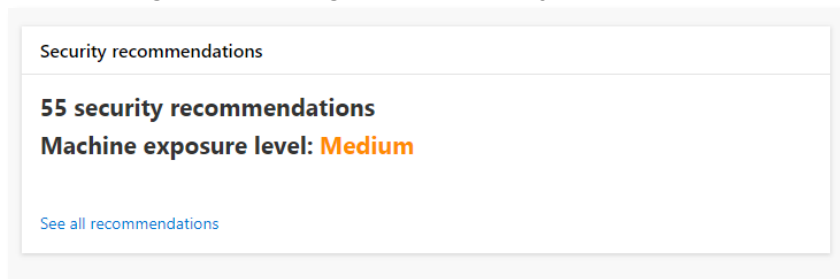
- [0-29] low exposure score
- [30-69] medium exposure score
- [70-100] high exposure score

You can view the individual machine exposure levels by navigating to a specific machine either by opening the dashboard's **Top exposed machine** widget or the **Exposure distribution** widget.

This scenario aims to reduce the exposure score of a machine in your organization to improve the overall organization exposure score.

Reduce your machine's threat and vulnerability exposure

1. Review the security recommendation of the selected machine by navigating to the machine page and clicking on the **Security recommendation** tab.




Note: There are two types of recommendations:

- *Security update* which refers to recommendations that require a package installation
- *Configuration change* which refers to recommendations that require a registry or GPO modification

2. Choose a recommendation that would be easy for you to apply. For example, a third-party tool that you can easily update, or a registry value that can be easily modified using *RegEdit*.



Note: Always prioritize recommendations that are associated with ongoing threats. These recommendations are marked with the  icon.

3. Connect to the machine and apply the selected recommendation.
4. Allow a few hours for the changes to propagate in the system.
5. Review the machine **Security recommendation** tab again. The recommendation should now disappear, and the exposure score should decrease.

Congratulations, you just reduced the exposure of the selected machine to internal and external threats!

The next step is to apply this recommendation on all the machines in your organization using your favorite security management tool, for example, Microsoft Security Center Configuration Manager (SCCM) or Microsoft Intune.

Doing so will reduce the overall organization exposure score based on the impact indicated in the recommendation.

Scenario 2: Remediation requests and monitoring

The Threat & Vulnerability Management capability in Microsoft Defender ATP bridges the gap between Security and IT Administrators through the remediation request workflow.

This capability allows you, the Security Administrator, to request for the IT Administrator to remediate a vulnerability or misconfiguration via Intune and SCCM.

Once requested, all the recommendation context (name, affected machines, justification, threat information) will generate a new security task in Microsoft Intune.

In addition to the prerequisites we've set in the beginning of this DIY, you should also:

- Onboard your machine to Intune or SCCM. If you are using SCCM, update your console to the latest May version 1905
- Tag or mark it as co-managed

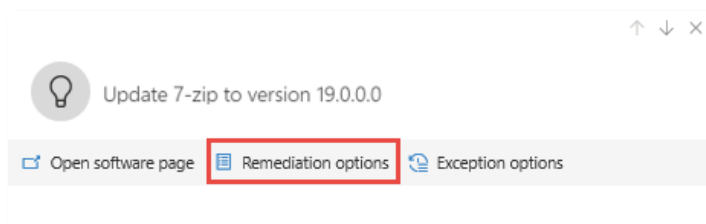


Note: To use this capability, enable your Microsoft Intune connections. Navigate to **Settings > General > Advanced features**. Scroll down and look for **Microsoft Intune connection**. By default, the toggle is turned off. Turn your **Microsoft Intune connection** toggle on.


☒ On Microsoft Intune connection
Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement. Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

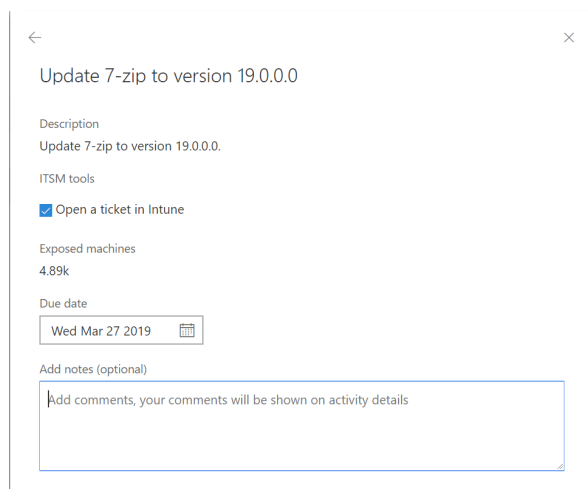
Request a remediation

1. Click on a security recommendation you would like to request remediation for, and then click **Remediation options**.



2. Select **Open a ticket in Intune (for AAD joined devices)**, select a due date, and optional notes for the IT Administrator. Then, click **Submit request**.

 **Note:** You also have the option to export all the data from the recommendation in the CSV format by selecting **Export all remediation activity data to CSV**.



Update 7-zip to version 19.0.0.0

Description
Update 7-zip to version 19.0.0.0.

ITSM tools
☒ Open a ticket in Intune

Exposed machines
4.89k

Due date
Wed Mar 27 2019

Add notes (optional)
Add comments, your comments will be shown on activity details

☐ Export all remediation activity data to CSV[Submit request](#)

That's it! Your ticket is on its way to the IT Administrator and waiting for their approval.

3. Notify your IT Administrator about the new request and have them log into Intune to approve or reject the request and start a package deployment.
4. View the status of the remediation request. Navigate to the remediation screen to view the activity progress

↑ ↓ ×

Update 7-zip to version 19.0.0.0

✓ Mark as completed ✕ Export to CSV

Remediation activity details

Description
Update 7-zip to version 19.0.0.0.

Started on	3/5/19
Status	In progress
Remaining time	19 days (4/2/19)
Completed on	-

Progress

0/4.83k

Completed

Scenario 3: Recommendation exception handling

Microsoft Defender ATP's TVM introduces a capability to create exceptions for recommendations, as an alternative to requesting for remediation.

There are various reasons why organizations might want to create exceptions for a recommendation. For example, a business or production need that prevents the company from applying the recommendation, the existence of a compensating or alternative control that provides the same level of protection that the recommendation would, a false positive, among other reasons.

Exceptions can be created for both *Security update* and *Configuration change* recommendations.

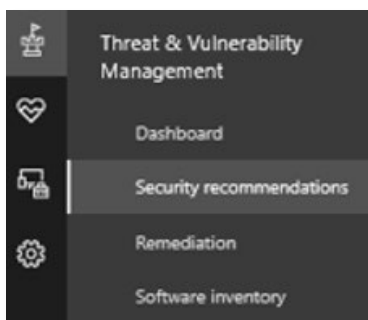
When an exception is created for a recommendation, the recommendation is no longer active. The recommendation state changes to **Exception**, and it no longer shows up in the security recommendations list.



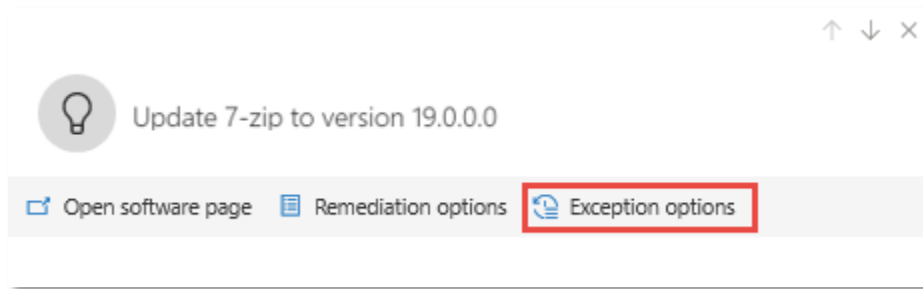
Note: You will still see the recommendations under exception by applying appropriate filters.

Creating an exception

1. Navigate to the **Security recommendations** page under the **Threat & Vulnerability Management** section menu.

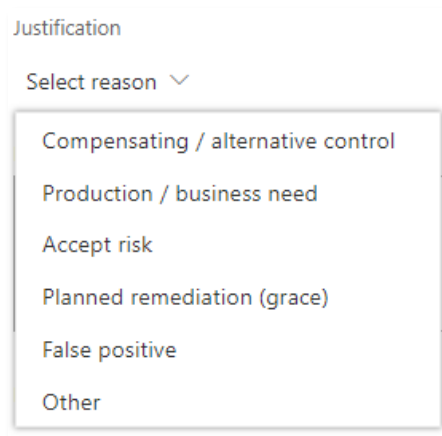


2. Click the top-most recommendation. A side panel will open with the recommendation details.
3. Click the **Exception options** button at the top of the side panel.

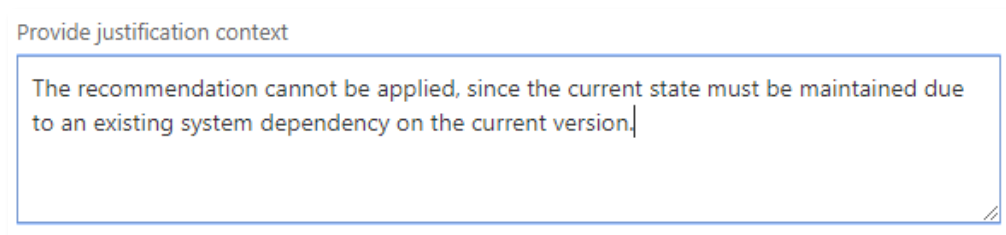


4. In the exception creation side panel, fill in the following details:

- **Justification** – the reason for creating the exception, chosen from a drop-down list



- **Justification context** – additional textual context related to the justification



- **Exception duration** – the period of time during which this exception will be in effect. When the exception expires, the recommendation automatically becomes active again

Exception duration

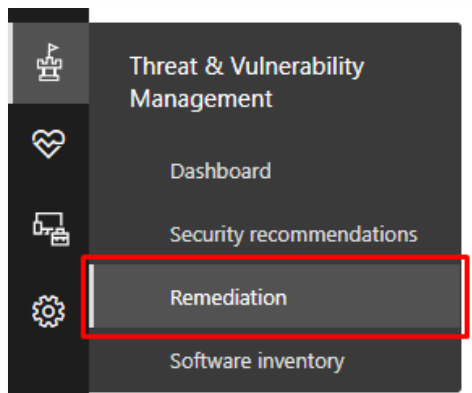
Set date ▾

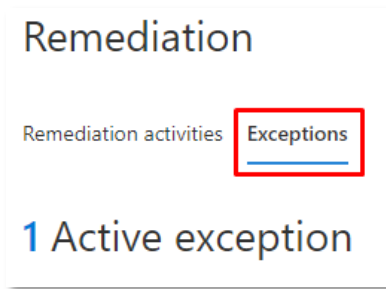
- 30 days
- 60 days
- 90 days
- Custom (up to 90 days)

5. Click **Submit**. A confirmation message at the top of the page will indicate that the exception has been created.

✓ Recommendation exception was created

6. View all your exceptions (current + past) by navigating to the **Remediation** page under the **Threat & Vulnerability Management** menu and clicking on the **Exceptions** tab.





7. Click the exception that you created to view the details.
8. Navigate again to the **Security recommendations** page under the **Threat & Vulnerability Management** menu – the recommendation will not appear there anymore as it is currently under exception.

Conclusion

We've walked you through how Microsoft Defender ATP's new Threat & Vulnerability Management capability can help you reduce your organization's threat and vulnerability exposure through discovery, prioritization, and remediation.

We've also shown you how easy it is to bridge the gap between the Security and IT Administration workflows by using this new capability.

We hope you enjoyed this simulation and are now encouraged to explore how you can apply this game-changing risk-based approach to your organization's security.

Click the feedback icon on the Microsoft Defender ATP portal to let us know how you feel about this simulation or any other aspects of the product. We would love to hear your ideas about additional simulations and tutorials. Thank you!

For information on getting started with Microsoft Defender ATP TVM see <https://aka.ms/mdatp-tvm>.