Filename: microsoft-ms101-7-3-1-implement-windows-defender-atp-policies
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Windows Defender Advanced Threat Protection (ATP)
EpisodeName: Implement Windows Defender ATP Policies
Description: Adam and Wes discuss how to implement Windows Defender ATP policies.

Implement Windows Defender ATP Policies

Implement Microsoft 365 Security and Threat Management (30-35%)

Implement Windows Defender Advanced Threat Protection (ATP)
• Plan Windows Defender ATP Solution
• Configure Preferences
• Implement Windows Defender ATP Policies
• Enable & Configure Security Features of Windows 10 Enterprise

==========

Implement Windows Defender ATP Policies

Onboarding clients can be done with the following tools:

```
• Microsoft Intune or another MDM
• System Center Configuration Manager (SCCM)
• Group Policy - NO AUTOMATED REPORTING; generate reports manually
• Script - provided by Microsoft, and useful for small deployments
```

How do I know a recently onboarded device is functional for Windows ATP?

POWERSHELL !!!! (run the following command with Administrative Permissions)

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden (New-Object
System.Net.Webclient).DownloadFile('http://127.0.0.1/1.exe','C:\test-WDATP-test\invoice.exe');Start-Process 'C:\test-WDATP-
test\invoice.exe'
```

OUTCOME: Ensure that an alert appears in the portal after the command is run

Online testing tools:
https://demo.wd.microsoft.com/?ocid=cx-wddocs-testground

How do I handle offboarding clients?

```
1. Download the offboarding package from the Windows Defender Security Center
```

site

```
2. Deploy the offboarding script using method of choice (GPO, Intune, SCCM or
```

manually run)

```
3. Validate that client offboarded successfully
```

FOR THE EXAM:

```
1. Offboarding package expires 30 days after download
2. After offboarding, client data remains available for 6 months
```

Troubleshooting issues:

```
3 possible health states for Windows Defender:

1. Active - HEALTHY !!!

2. Misconfigured - Something(s) needs fixin'

3. Inactive - Clients NOT REPORTING in for 7 days or longer; also if the O/S
```

is reinstalled

Windows events in the Operational Log to look out for:

PATH - Applications and Services logs\Microsoft\Windows\SENSE\Operational

```
• Client onboarded successfully (event ID 11)
• Client did not onboard successfully (event ID 6, 10, 25 & 26)
• Windows ATP service did not start (event ID 3)
```

Review events and errors using Event Viewer:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/event-error-codes