Microsoft

WELCOME TO

FastTrack Partner Office Hours

Presenters: Matt Novitsch, Daniel Selleri, Phillip Gerdes

Audience: FastTrack Partner Community

February 2025

Microsoft

Agenda

- ✓ Device Control with Defender for Endpoint and Intune
- ✓ Defender on Linux – Deployment overview, tips and tricks
- ✓ ADG – Advanced Deployment Model
- ✓ SME Request process
- ✓ Q&A

Device Control with Defender for Endpoint and Intune

Presenter: Matt Novitsch

Device control in Microsoft Defender for Endpoint

Device control capabilities in Microsoft Defender for Endpoint enable your security team to control whether users can install and use peripheral devices, like removable storage (USB thumb drives, CDs, disks, etc.), printers, Bluetooth devices, or other devices with their computers. Your security team can configure device control policies to configure rules like these:

- Prevent users from installing and using certain devices (like USB drives)
- Prevent users from installing and using any external devices with specific exceptions
- Allow users to install and use specific devices
- Allow users to install and use only BitLocker-encrypted devices with Windows computers

What's in it for me?

The benefits include…	To address…
Preventing unauthorized devices from being used on your corporate devices.	Simplifying the customer journey and drive deployment of the product
Preventing users from printing on non-approved devices.	Ensuring corporate data is not printed outside the corporate environment

Reference Links

- Deploy and manage device control in Microsoft Defender for Endpoint with Group Policy
- Deploy and manage device control in Microsoft Defender for Endpoint with Microsoft Intune
- View device control events and information in Microsoft Defender for Endpoint
- Device control in Microsoft Defender for Endpoint
- Information for Developers | USB-IF
- Intune endpoint security disk encryption policy settings
- https://Aka.ms/MattNovitsch

Demo

Microsoft

Defender on Linux

Presenter: Daniel Selleri

FastTrack benefit: Service Description

MDE Service Description summary

In Scope	Out of Scope
✓ Assessing **operating system version** and device management approach ✓ Planning for **network communications**, including proxies and firewalls ✓ Reviewing use of **MDE Plan 1 and Plan 2** features that apply to Linux ✓ **Onboarding** of Linux servers to **MDE using manual methods**, limited to Linux server distributions supported by MDE ✓ Creating **MDE policies** and preferences using local configuration files or Defender Security Settings Management ✓ **Targeting of policies** and preferences using groups and tags Review use of core MDE on Linux tools: command line interface, configuration analyzer, performance analyzer	× Linux instances with **customized kernels**. × Prescriptive assistance with any **non-Microsoft systems management tools** or development of configuration files associated with these tools, such as those listed below. FastTrack will refer customers to applicable technical guidance for these tools. × Chef, Puppet, Ansible, Saltstack × Enablement or management guidance for **Windows Subsystem for Linux** and **Windows Subsystem for Linux plugin** on Windows clients × **Troubleshooting** of MDE onboarding, management, configuration, and performance. FastTrack will direct customers to Microsoft Support for assistance with

Reference:

- ✓ Microsoft FastTrack – Defender XDR Service description
- ✓ Microsoft Defender for Endpoint on Linux
- ✓ Deploy Microsoft Defender for Endpoint on Linux manually, using Puppet, Chef, Ansible, Saltstack

Typical Engagement – Initial timeline

Week	Phase	Activity milestones	Resources
Week 1	Kickoff & discovery	Introduction, review Products capabilities, determine objectives, set meeting cadence	Executive sponsor, PM
		Overview of prerequisites, background and environment discovery.	
		Review deployment & onboarding methodology (Manual, Ansible, Chef, MDC, etc.)	
		Review connectivity requirements	
		Review FAQs	
Week 2 - 3	Configuration	Identify Servers for Pilot and create Dynamic Device Groups, enable enforcement scope	Endpoint Security Manager, Security Admins
		Create an asset rule, create security groups, create an AV Policy, create an EDR policy	
		Defender portal overview, review XDR Unified RBAC, create device group, review remediation levels	Endpoint Security Manager, SOC team, Linux Server Admins
		Deploy 1-5 pilot machines and validate the onboarding process	
		Review update process, if necessary, schedule MDE application update	
Week 4	Monitoring & actions	Test / Create an incident to validate	Linux Server Admins, Security Admins
		Overview of Security Posture	
		Overview of Defender for Endpoint Vulnerability Management (TVM)	
		Overview of Investigation (incidents and alerts)	
		Overview of Device actions and inventory	
		Defender Report analysis (device health & OS, Microsoft Defender AV health)	
	Pilot closure & next steps	Learnings, recommendations and deployment strategy	PM, Executive sponsor

Reference:

✓ Microsoft FastTrack – Defender XDR Service description

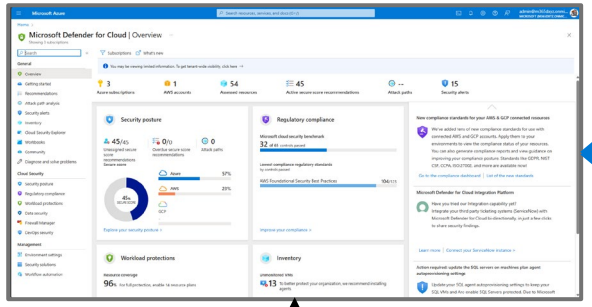
Kickoff Discovery Questions

- ✓ Industry
- ✓ Total Linux servers
- ✓ What Linux distributions and versions do you have?
- ✓ What anti-virus solution do you currently have to protect Linux servers?
- ✓ What is the total # of current MDE Linux deployments?
- ✓ Have you tried MDE Linux already?
- ✓ What is your experience with MDE? Windows 10/11? Windows Servers?
- ✓ Where are your Linux servers located? <on prem? Azure? AWS?
- ✓ Total types of **servers**: Ephemeral (persistent) vs non-ephemeral (non-persistent) vs containers
- ✓ Are there any asks/blockers/deal breakers that you have raised in the past for MDE Linux?

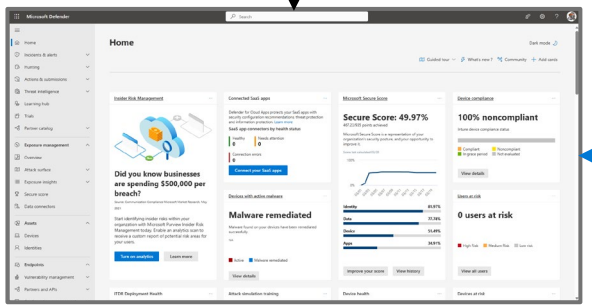
Reference:

- ✓ Microsoft Defender for Endpoint on Linux
- ✓ Onboard servers to the Microsoft Defender for Endpoint service
- ✓ Deploy Microsoft Defender for Endpoint on Linux manually, using Puppet, Chef, Ansible, Saltstack

MDC – Onboarding Method for Linux Servers



Defender for Cloud portal



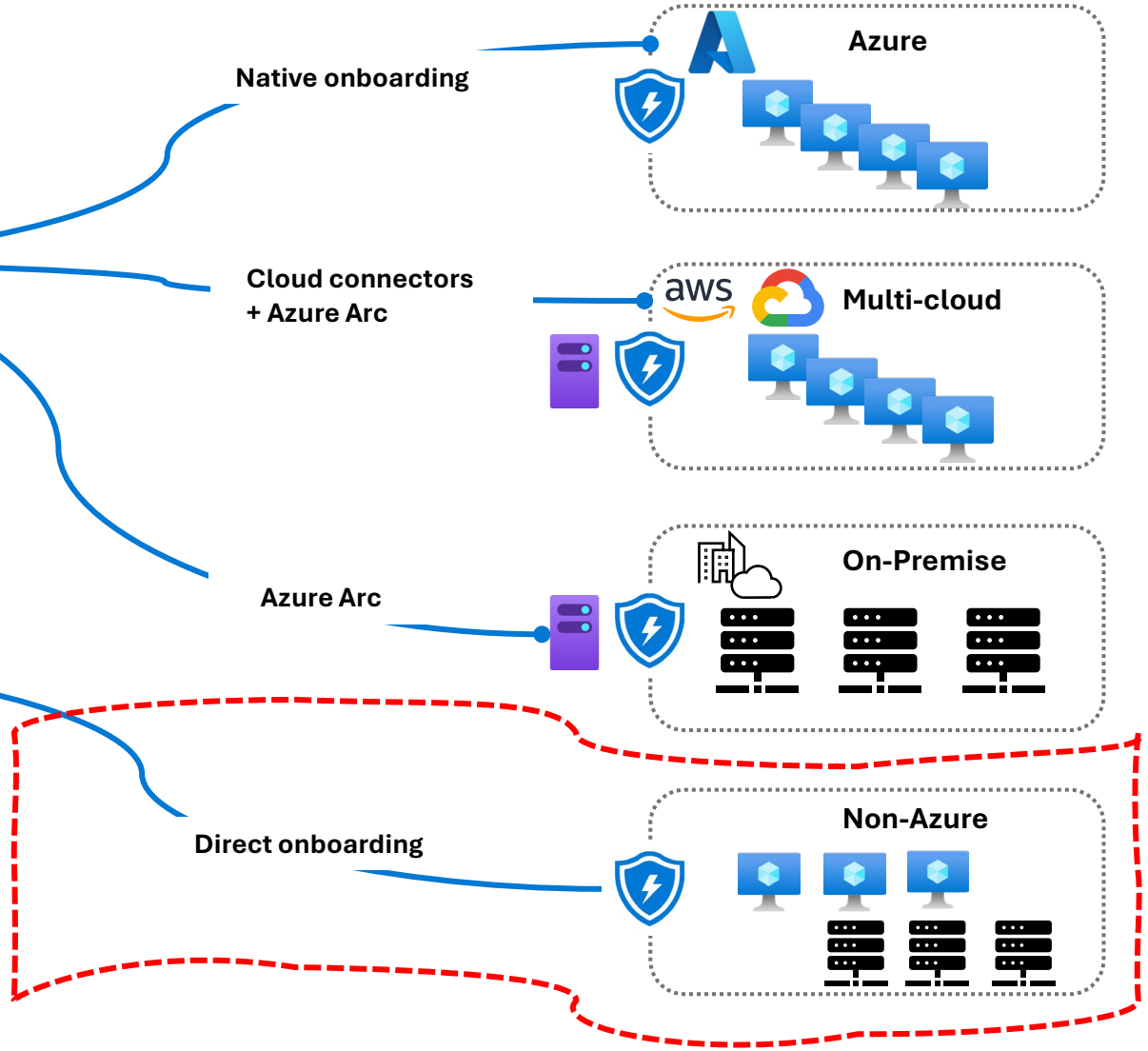
M365D portal

Native onboarding

Cloud connectors + Azure Arc

Azure Arc

Direct onboarding



Reference:

- ✓ Microsoft Defender for Endpoint on Linux
- ✓ Onboard servers to the Microsoft Defender for Endpoint service

Agent Update

Automatically Managed by Defender for cloud

Microsoft Defender for Servers Plan 2

Plan details

- Microsoft Defender for Endpoint
- Microsoft Defender vulnerability management
- Automatic agent onboarding, alert and data integration
- Generates detailed, context-based, security alerts easily integrated with any SIEM
- Provides guidelines to help investigate and mitigate identified threats
- Agentless VM vulnerability scanning Learn more.
- Agentless VM secrets scanning Learn more.
- Agentless malware detection
- Control plane security alerts
- Resolve missing software updates gaps with Azure Update Manager (Free for Plan 2 Arc machines)
- Regulatory compliance and industry best practices
- Just-in-time VM access for management ports
- Network layer threat detection
- File integrity monitoring
- Baselines assessment
- Log Analytics 500MB free data ingestion

Manual or automating via 3rd party / crontab

To set cron jobs in Ansible

```
Bash
cron - Manage cron.d and crontab entries
```

See https://docs.ansible.com/ansible/latest for more information.

To set crontabs in Chef

```
Bash
cron resource
```

See https://docs.chef.io/resources/cron/ for more information.

To set cron jobs in Puppet

See https://puppet.com/docs/puppet/5.5/types/cron.html for more information.
Automating with Puppet: Cron jobs and scheduled tasks
See https://puppet.com/blog/automating-puppet-cron-jobs-and-scheduled-tasks/

Crontab syntax

```
CRON_TZ=America/Los_Angeles
* 5 * * 0  sudo apt-get install –only-upgrade mdatp >> /tmp/mdatp_cron_job.log
```

Field	Time Unit	
1	Minute	0 - 59
2	Hour	0 - 23
3	Day of the month	1 - 31
4	Month	1 - 12
5	Day of the week	0 - 7 (0 & 7 is Sunday)

"Run following command on Sunday every month 5:00 AM at US, Los Angels time sudo apt-get install –only-upgrade mdatp >> ~/mdatp_cron_job.log"

3rd party tool to check the expressions
Cron Expression Examples - Crontab.guru

Life cycle

Each version of Defender for Endpoint on Linux is set to expire automatically after 9 months.
Customer to balance new functionalities vs. timeline to update

Reference:

- ✓ Remediate system updates and patches recommendations
- ✓ Overview of Defender for Servers in Microsoft Defender for Cloud
- ✓ How to schedule an update for Microsoft Defender for Endpoint on Linux
- ✓ Deploy updates for Microsoft Defender for Endpoint on Linux

AuditD and eBPF Support

- ✓ eBPF

  Starting with version 101.24082.0004, MDE on Linux no longer supports the AuditD event provider. We're transitioning completely to the more efficient extended Berkeley Packet Filter (eBPF) technology.

- ✓ AuditD

  If eBPF isn't supported, or if there are specific requirements make sure Defender for Endpoint on Linux version 101.24072.0001 or lower.

- ✓ In case you want to manually disable eBPF

```bash
sudo mdatp config ebpf-supplementary-event-provider --value [enabled/disabled]
```

```
danielsa@srv072:~$ mdatp health
healthy                                          : true
health_issues                                    : []
licensed                                         : true
engine_version                                   : "1.1.24090.13"
engine_load_status                               : "Engine not loaded"
app_version                                      : "101.24092.0002"
org_id                                           : "2bd20459-d376-4e57-abe8-175a9d1e7237"
log_level                                        : "info"
machine_guid                                     : "9f4c746c-57ec-824e-8bc6-fe3c9d8d263d"
release_ring                                     : "Production"
product_expiration                               : Jul 17, 2025 at 11:49:56 PM
cloud_enabled                                    : true [managed]
cloud_automatic_sample_submission_consent        : "safe" [managed]
cloud_diagnostic_enabled                         : true [managed]
cloud_pin_certificate_thumbs                     : false
passive_mode_enabled                             : true [managed]
behavior_monitoring                              : "disabled" [managed]
real_time_protection_enabled                     : false [managed]
real_time_protection_available                   : true
real_time_protection_subsystem                   : "fanotify"
supplementary_events_subsystem                   : "ebpf"
automatic_definition_update_enabled              : true [managed]
definitions_updated                              : Feb 07, 2025 at 06:33:30 AM
definitions_updated_minutes_ago                  : 4488
definitions_version                              : "1.421.1751.0"
definitions_status                               : "up_to_date"
edr_early_preview_enabled                        : "disabled"
edr_device_tags                                  : [{"key":"GROUP","value":"MDE-Management"}]
edr_group_ids                                    : ""
edr_configuration_version                        : "30.199999.main.2025.02.04.04-F4E3390C426C
edr_machine_id                                   : "6dd8f8641d454daf9cb1169612bdbde113de49e2"
managed_by                                       : "MDE"
conflicting_applications                         : []
network_protection_status                        : "stopped"
network_protection_enforcement_level             : "disabled" [managed]
danielsa@srv072:~$
```

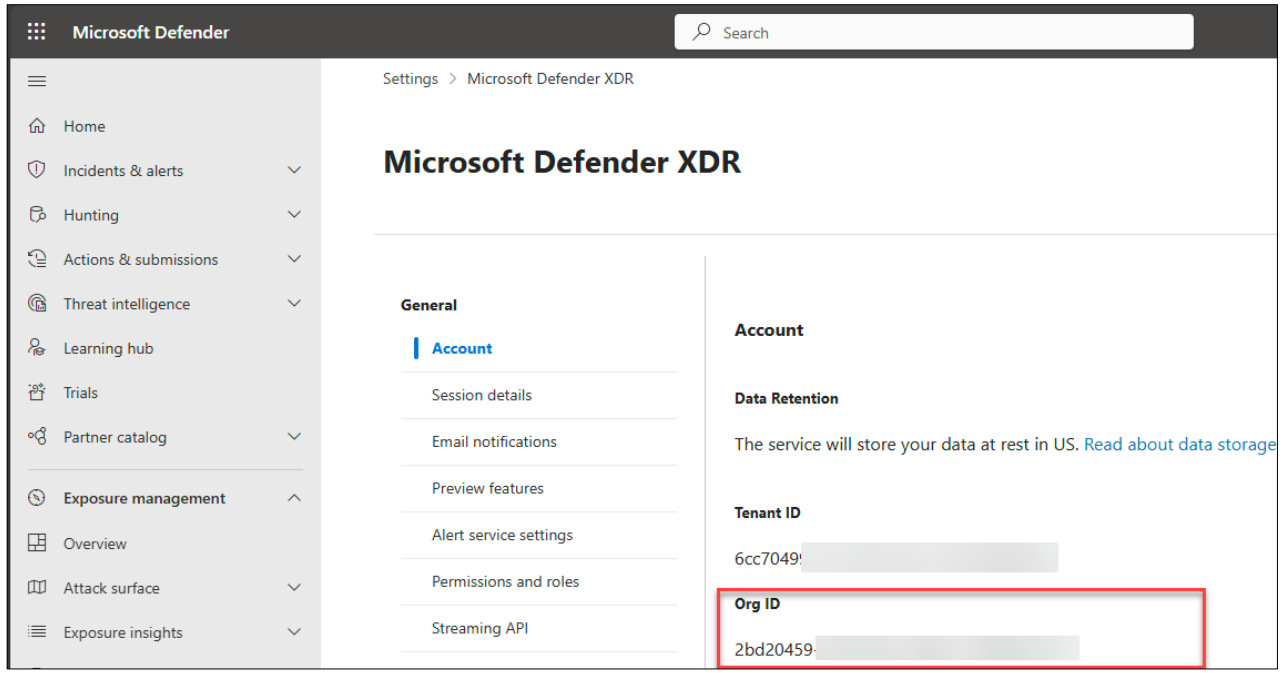
Reference:

- ✓ Microsoft Defender for Endpoint on Linux
- ✓ Troubleshoot performance issues for Microsoft Defender for Endpoint on Linux
- ✓ Use eBPF-based sensor for Microsoft Defender for Endpoint on Linux

Network Protection

Prerequisites

- ✓ License (can be trial)
- ✓ MDE on Linux version 101.78.13 or later
- ✓ Insiders-Slow or Insiders-Fast channel
- ✓ Send e-mail to: xplatpreviewsupport@microsoft.com
  - ✓ Add your Org ID number into the e-mail




```
danielsa@srv072:~$ mdatp health
healthy                 : false
health_issues           : ["Network Protection cannot start due to unsupported release ring"]
licensed                : true
engine_version          : "1.1.24090.13"
engine_load_status      : "Engine not loaded"
app_version             : "101.24092.0002"
org_id                  : "2bd20459-d376-4e57-abe8-175a9d1e7237"
log_level               : "info"
machine_guid            : "9f4c746c-57ec-824e-8bc6-fe3c9d8d263d"
release_ring            : "InsiderFast"
product_expiration      : Jul 17, 2025 at 11:49:56 PM
cloud_enabled           : true [managed]
```

Don’t forget to send the e-mail

Reference:

- ✓ Network protection for Linux

Security Management

Phase 01: Pilot

- ✓ Enable Linux devices enforcement scope to “tagged devices”
- ✓ Create a Dynamic / Static group on Microsoft Entra
- ✓ Add the “MDE-Management” to the server
  - ✓ Manual Tag
  - ✓ json file
  - ✓ Command line

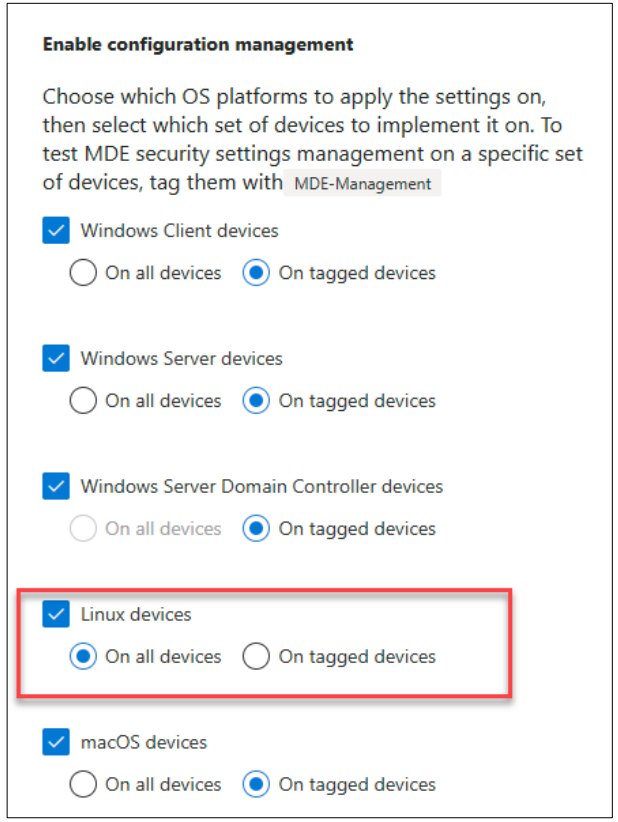
    sudo mdatp edr tag set --name GROUP --value MDE-Management
  - ✓ Create an EDR policy (Optional)

```
danielsa@srv072:~$ sudo mdatp edr tag set --
name GROUP --value MDE-Management
This setting is managed by your organization
danielsa@srv072:~$
```

> ⓘ **Important**
>
> Use of dynamic device tagging capabilities in Defender for Endpoint to tag devices with `MDE-Management` isn't currently supported with security settings management. Devices tagged through this capability don't successfully enroll. This is currently under investigation.

Phase 02: Going at scale

- ✓ Remove the used configuration for the Pilot
- ✓ Change:
  - ✓ Linux devices enforcement scope to “all devices”



Reference:

- ✓ Learn about using Intune to manage Microsoft Defender settings on devices that aren't enrolled with Intune
- ✓ Create dynamic rules for devices in asset rule management

Network / SSL Inspection

Network connectivity

- ✓ Traffic for Defender for Endpoint should NOT be inspected by SSL inspection (TLS inspection).
- ✓ To allow connectivity to the consolidated set of URLs or IP addresses, ensure your devices are running the latest component versions.
- ✓ Run: mdatp connectivity test

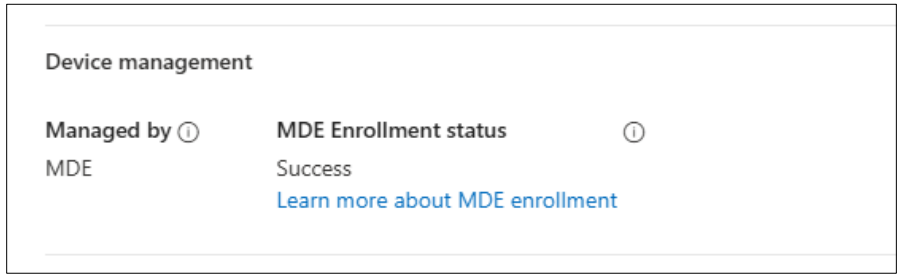
```
danielsa@srv072:~$ mdatp connectivity test
Testing connection with https://nf.smartscreen.microsoft.com/api/network/mac ... [OK]
Testing connection with https://unitedstates.smartscreen-prod.microsoft.com//api/network/mac ... [OK]
Testing connection with https://unitedstates.smartscreen.microsoft.com//api/network/mac ... [OK]
Testing connection with https://mdav.us.endpoint.security.microsoft.com/mdav/test ... [OK]
Testing connection with https://mdav.us.endpoint.security.microsoft.com/storage/ussusleastprod/ ... [OK]
Testing connection with https://mdav.us.endpoint.security.microsoft.com/storage/ussuslwestprod/ ... [OK]
Testing connection with https://mdav.us.endpoint.security.microsoft.com/xplat/api/report ... [OK]
Testing connection with https://mdav.us.endpoint.security.microsoft.com/packages/?ostype=linux ... [OK]
Testing connection with https://discovery.dm.microsoft.com/enrollmentConfiguration/discovery/atp ... [OK]
Testing connection with https://edr-cus.us.endpoint.security.microsoft.com/edr/commands/test ... [OK]
Testing connection with https://edr-eus.us.endpoint.security.microsoft.com/edr/commands/test ... [OK]
Testing connection with https://edr-cus3.us.endpoint.security.microsoft.com/edr/commands/test ... [OK]
Testing connection with https://edr-eus3.us.endpoint.security.microsoft.com/edr/commands/test ... [OK]
Testing connection with https://us-v20.events.endpoint.security.microsoft.com/ping ... [OK]
Testing connection with https://edr-cus.us.endpoint.security.microsoft.com/storage/automatedirstrprdcus/ ... [OK]
Testing connection with https://edr-eus.us.endpoint.security.microsoft.com/storage/automatedirstrprdeus/ ... [OK]
Testing connection with https://edr-cus3.us.endpoint.security.microsoft.com/storage/automatedirstrprdcus3/ ... [OK]
Testing connection with https://edr-eus3.us.endpoint.security.microsoft.com/storage/automatedirstrprdeus3/ ... [OK]
danielsa@srv072:~$
```

Quick check before troubleshooting

If the network connectivity test does not fail, check the console before start advanced troubleshooting

E.g., You have configured the Security Settings and still not seeing the synthetic computer object after 24 hours.

- ✓ Under device properties
  - ✓ MDE Enrollment status as **limited connectivity**



Reference:

- ✓ Troubleshoot cloud connectivity issues for Microsoft Defender for Endpoint on Linux
- ✓ Onboarding devices using streamlined connectivity for Microsoft Defender for Endpoint
- ✓ Troubleshoot onboarding issues related to Security Management for Microsoft Defender for Endpoint

Recommended AV policies

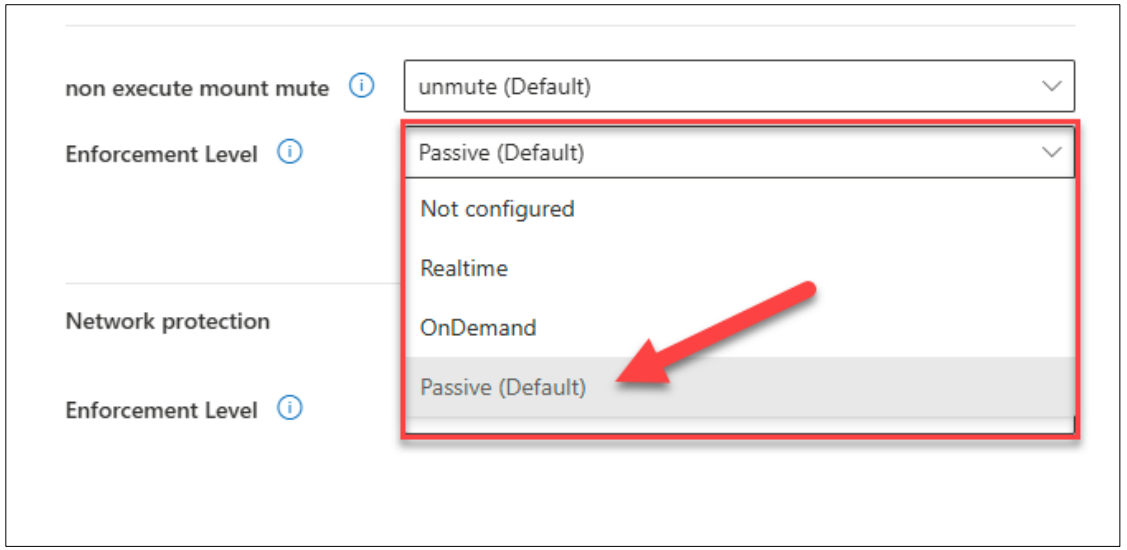
Initial deployment / Pilot

Group servers per role

- ✓ Group servers based on the profile / role

- ✓ Start with the “sample profile” or use the default values
- ✓ Review the “Common mistakes to avoid”
- ✓ Apply the vendor recommendation (e.g., SAP, Database)
- ✓ Customize and validate the exclusions

The default configuration “balance” the security and performance impact. Review the policy after the pilot.
E.g., Enforcement Level as passive



Reference:

- ✓ Set preferences for Microsoft Defender for Endpoint on Linux
- ✓ Common mistakes to avoid when defining exclusions
- ✓ Configure and validate exclusions for Microsoft Defender for Endpoint on Linux

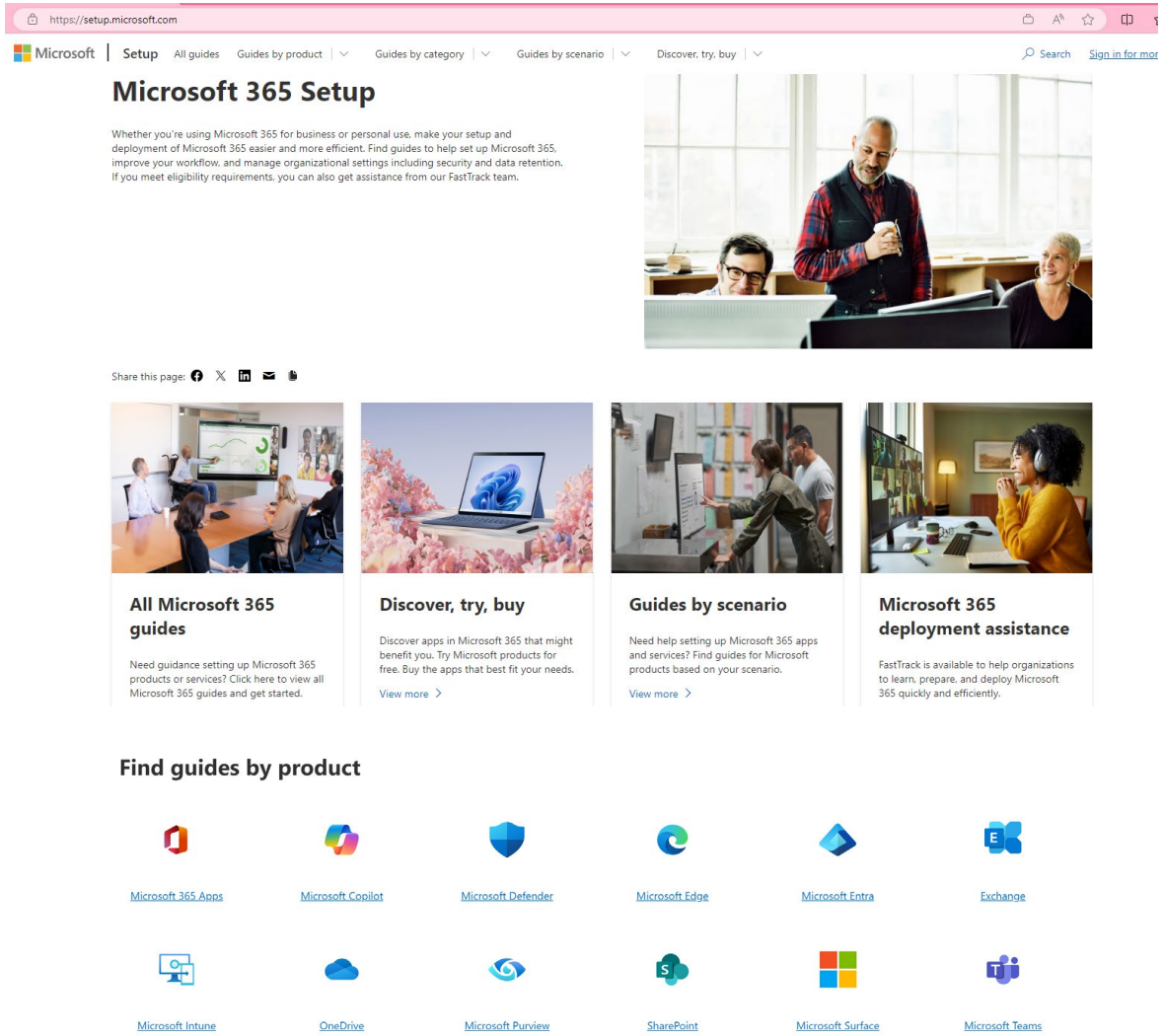
Microsoft

ADG – Advanced Deployment Guide

Presenter: Phillip Gerdes

FastTrack M365 Advanced Deployment Guides

A consistent FastTrack experience to help take customers from foundational to advanced enablement and help them realize the full potential of their investment



What are they?

- **Simplified** guidance and processes available in the Microsoft 365 admin center to deploy workloads.

Why are they important?

- FastTrack Ready Partners and FastTrack Managers use them to **establish a clear deployment roadmap, scope, and expectations** of the FastTrack benefit.
- This repeatable tool **helps to improve the consistency** of the service that the customer experiences.
- **FastTrack services are more easily explained** when a customer can visually see the deployment path.

M365 Advanced Deployment Guides

Advanced Deployment Guides

Tailored guidance and resources for planning and deploying.

62 Advanced Deployment Guides covering identity, security, device management, productivity, collaboration & voice, and employee experience.

Provides **setup survey, prerequisites, feature & policy configuration and deployment**, and reporting.

Integrated M365 deployment strategy covering configure scenarios, adoption scenarios, compliance score, & secure score.

Microsoft's latest recommended deployment rollout strategy & best practices:

- Access to deployment best practices upfront in one centralized format
- Centralized resources to MS documentation & videos
- Mapped deployment scenarios
- Automated deployment steps
- Hydrations back to tenant showing licensing
- Project tracking capabilities

How to Deliver

Self-Service Tool

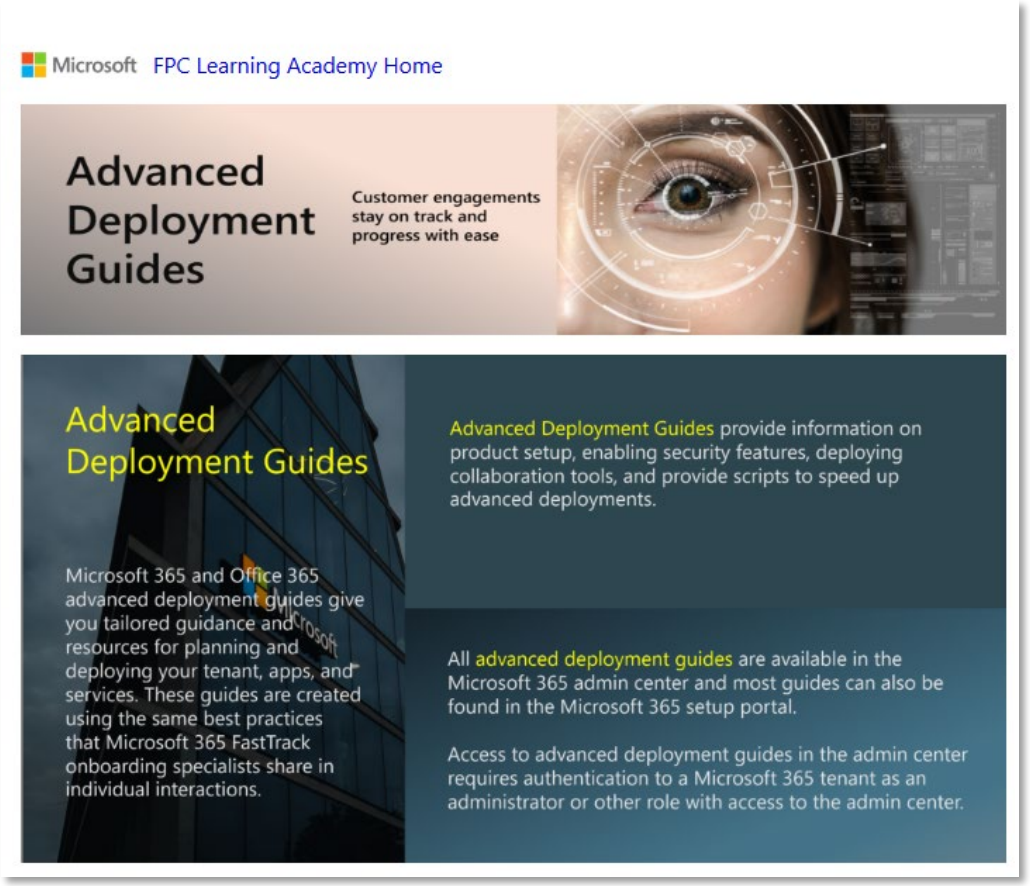
- Greenfield deployment strategy: use as M365 deployment roadmap for customer
- Customer refers to as deployment aid & resource hub
- Project tracking tool Deployment scenarios

Expanding Engagement

- Uncover cross-workload deployment dependencies and connect across M365 suite
- Build intent:
  - Introduce new workloads
  - Spark existing customer curiosity with ability to easily present a complete deployment plan
  - Renewal +upsell and try & buy
- Segway into value-added service conversations such as adoption
- Include in proactive marketing campaign emails or
- Leverage data in FRP Insights to view ADG interaction & use as propensity for deployment indicator.

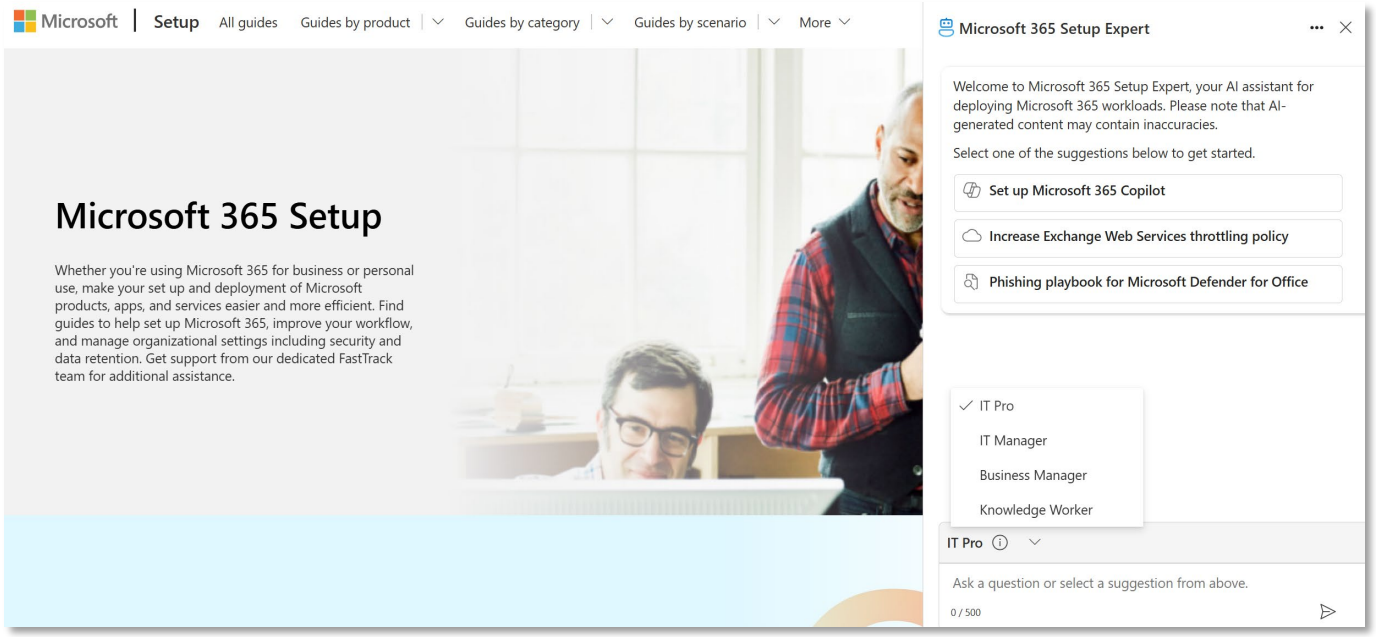
ADG Learning Resources

FPC Academy



[KB-01579 · FastTrack Partner Community Portal]

Setup Expert



[Microsoft 365 Deployment Guides and Setup Wizards | Microsoft 365 Apps]

SME Request Process

SME Request Portal: FastTrack Assistance Center (powerappsportals.com)

SME Requests - What to Expect

Designated SMEs support deployment, answer questions, and provide training within our OKR WLs

Designated FE	Designated Partner SME				
	Teams & Teams Phone	Viva	Security / Identity	Purview	InTune Desktop

Best Practices and Guidelines

- Our Designated SMEs aim to make contact within 3 days of assignment.
- For any break/fix issues, please contact the support team instead of sending requests.
- Designated SMEs help resolve deployment challenges; not for staff augmentation.
- Please provide a clear and concise description of your situation and needs for a faster response.
- Please limit each request to one topic or product.
- We value your feedback and suggestions for improving our products.

Benefits

- Streamline process
- Provide a faster Resolution
- Have a better understanding of technical issues partners face.
- Influence Microsoft products

Q&A

Microsoft

Thank you