Edge Management Service
- The modern way to manage Edge

Jörgen Nilsson & Ronni Pedersen

Jörgen Nilsson
Microsoft MVP · Security & Windows

Role
Trusted Advisor, Onevinn

Focus
Intune · Security · Windows · Windows 365

Blog, Hobbies and more
BBQ
Ccmexec.com

Ronni Pedersen

Microsoft MVP · Security & Windows

Role

Senior Cloud Architect, Apento

Focus

Intune · Security · Windows · AI · Compliance

Blog, Hobbies and more

BBQ, Hiking

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

Agenda

- Introduction
- Edge Management Service
- Extensions
- Security Baselines
- Migration from Intune/Group Policy
- Multi-platform support
- B2B & BYOD

Browsers – our most important app

- Number of SaaS applications used per organisation has increased every year, but we are seeing consolidation of SaaS apps as a trend.
- With SaaS apps becoming more and more important when CRM, Finance and many other systems moved to the Web, Browser security is more important than ever!
- How is our browser secured?
- BYOD access to webapps?
- How are they secured?
- Extensions how secure are they?

Browser strategy

From ServiceDesk ticket:

“The xxx webpage doesn’t work in Edge and we must complete this month’s salary payment ASAP”

Customer update:

“This is not urgent anymore as it worked in Firefox”

The root cause was an expired certificate!!

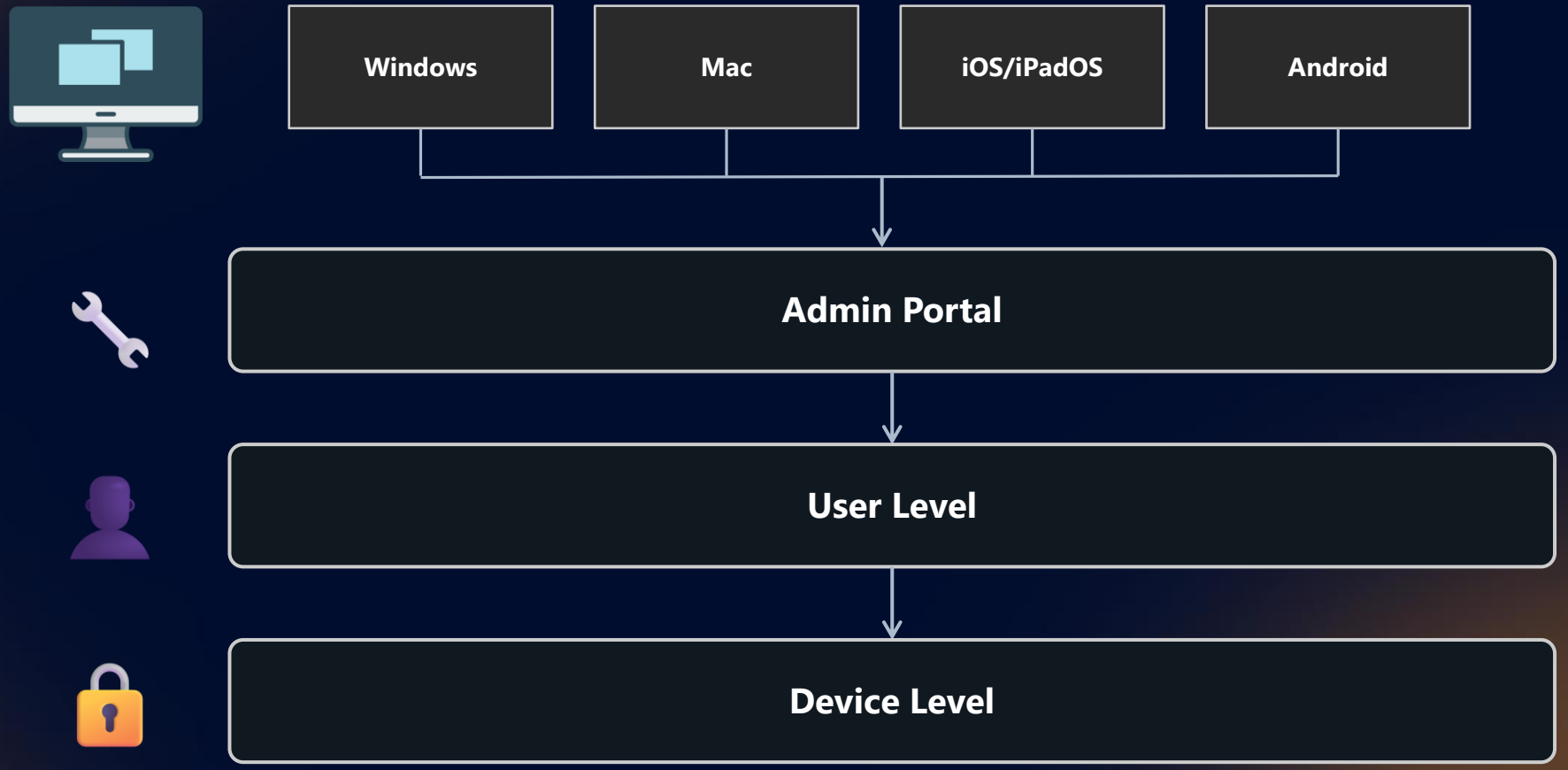
- How secure is Firefox when you can bypass security features?

Edge Management Service

- Admin.Microsoft.com portal
- Microsoft Edge Administrator - Role
- A single pane of glass for Edge management Cloud+Intune
- **Priority!**
- Zero-day support for new settings

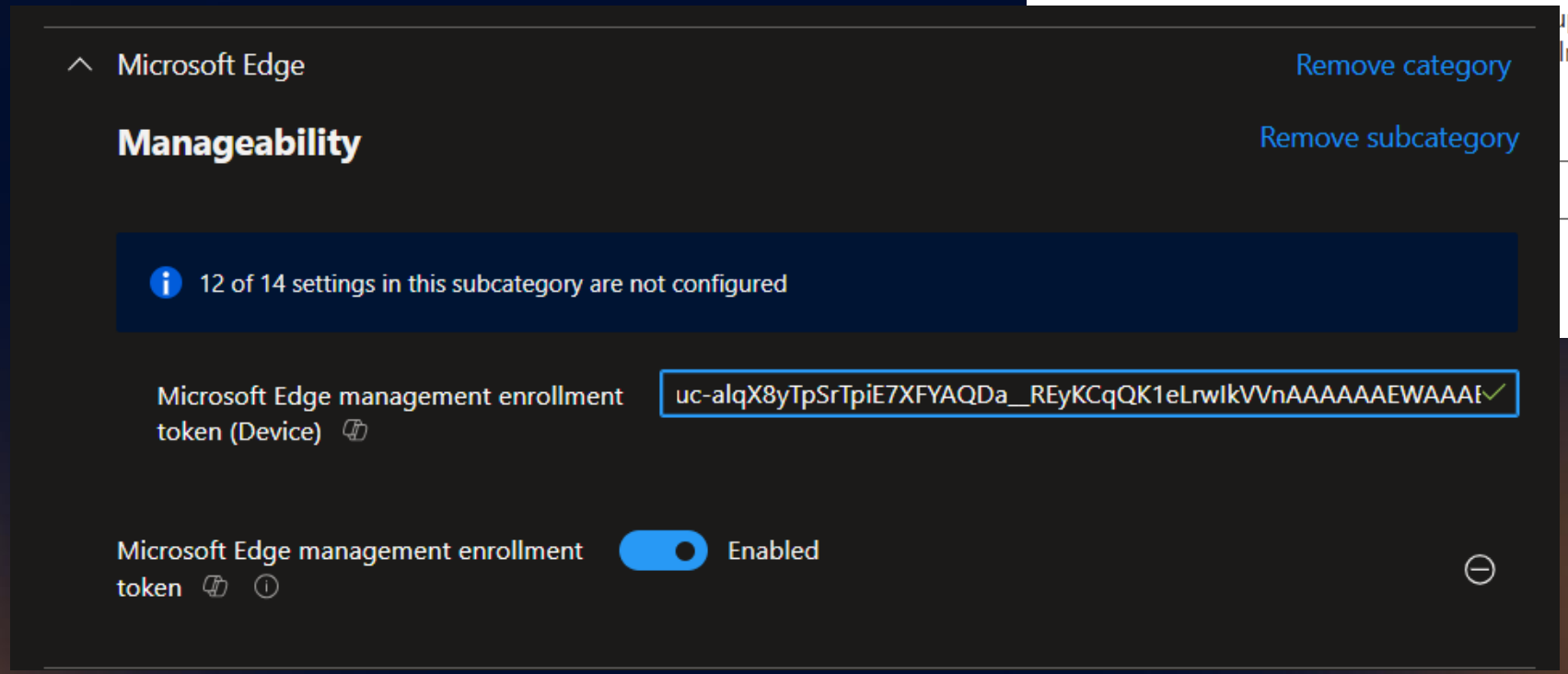
☐	NA	Win - Conflict 2
☐	NA	Win - Conflict 1
☐	NA	Edge conflict
☐	0	Security Baseline
☐	1	Security Settings
☐	2	Edge Standard
☐	3	Security baseline v128
☐	4	Edge Demo
☐	5	Show Home button
☐	6	Monitoring Policy This policy was auto-created from the monitoring pa policy, visit the monitoring page.
☐	7	Configure Extensions
☐	8	Purview browser protections policy for Unmanag blocks other non-compliant browsers

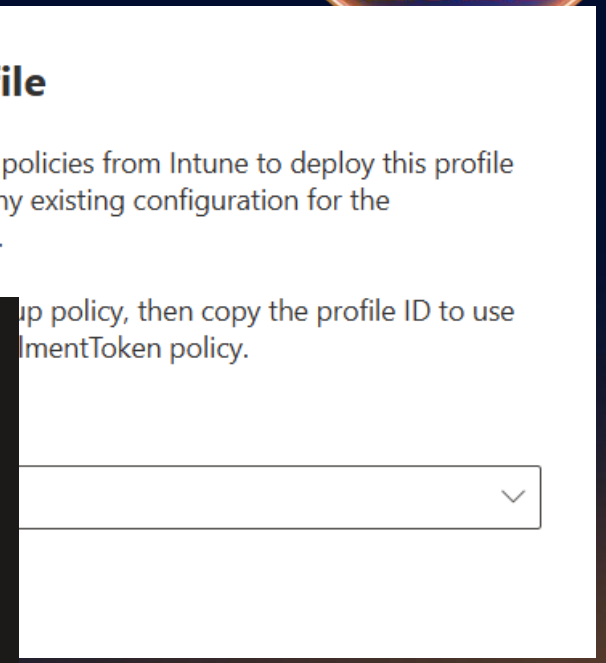
Edge Management Service



Targeting

- User Sign in to Edge = Per Tab!
- Enrolment token = Per Device (Windows only)





Monitoring (Default)

Policies for Microsoft Edge

Overview | Configuration policies | Site lists | Connectors | **Monitoring dashboard** | Provide Feedback

Devices recommended to update
10 *out of 11*

Requested extensions
8

Requested IE mode sites
0

Ensuring all devices are running the latest Edge version improves your overall security posture. The following tables provide details about Edge versions running in your organization and actions you can take to keep them up to date. View these details by turning on the toggle to enable version monitoring. Note: If you have set Edge update policies for your organization, this feature may not work as expected.

Enable version monitoring

Edge version management

Edge update status

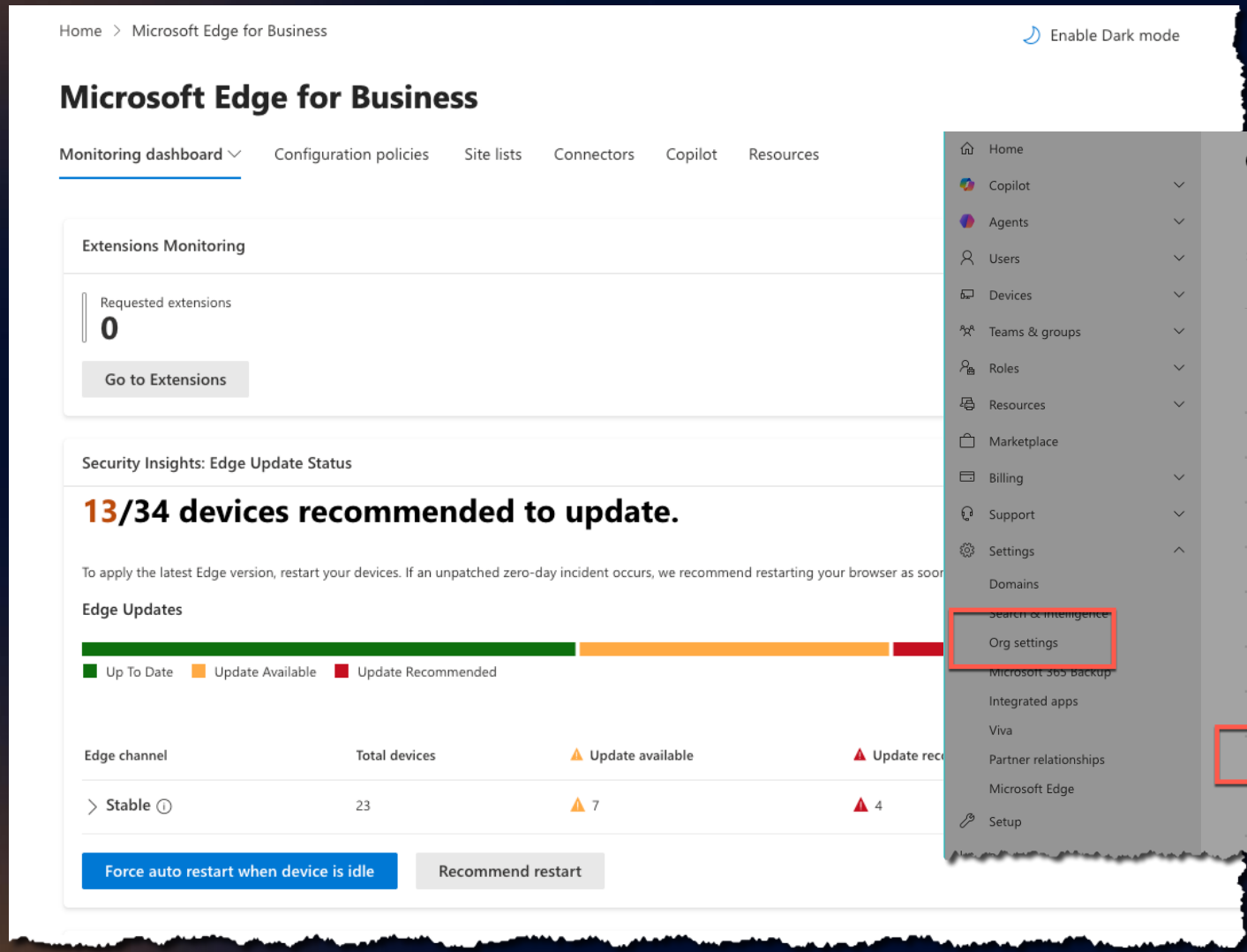
11 total managed devices, 1 devices sending data in the last 24 hours.

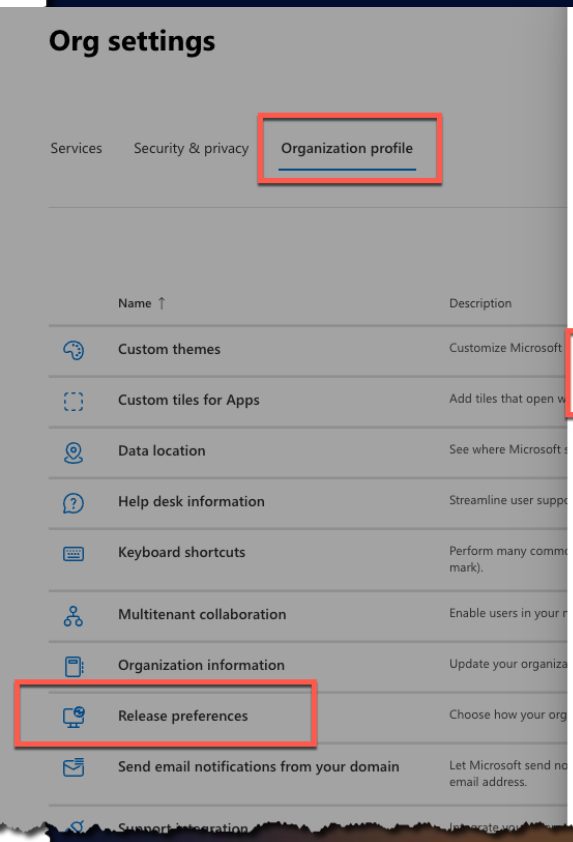
Devices without the latest Edge updates may be vulnerable. We recommend restarting these instances to apply the latest browser version. In the event of an unpatched zero-day incident, we strongly suggest restarting the browser as soon as a security update is released.

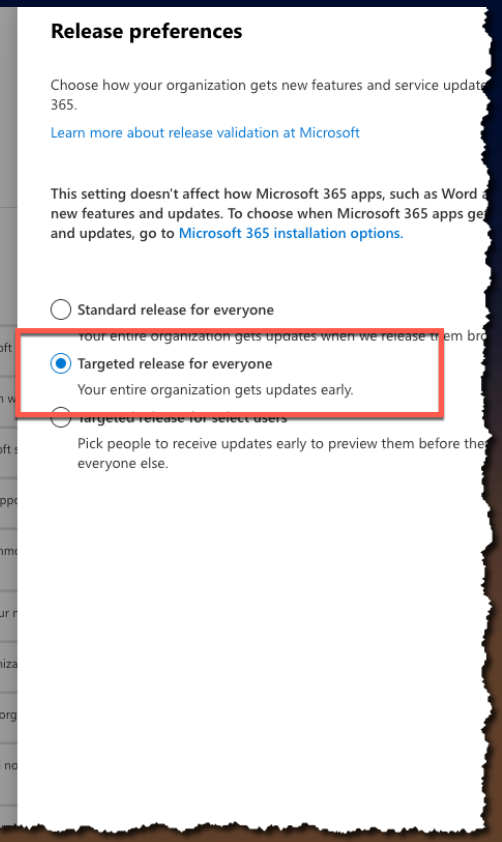
Updated at September 8, 2025 at 9:38 PM today

Up To Date | Update Available | Update Recommended

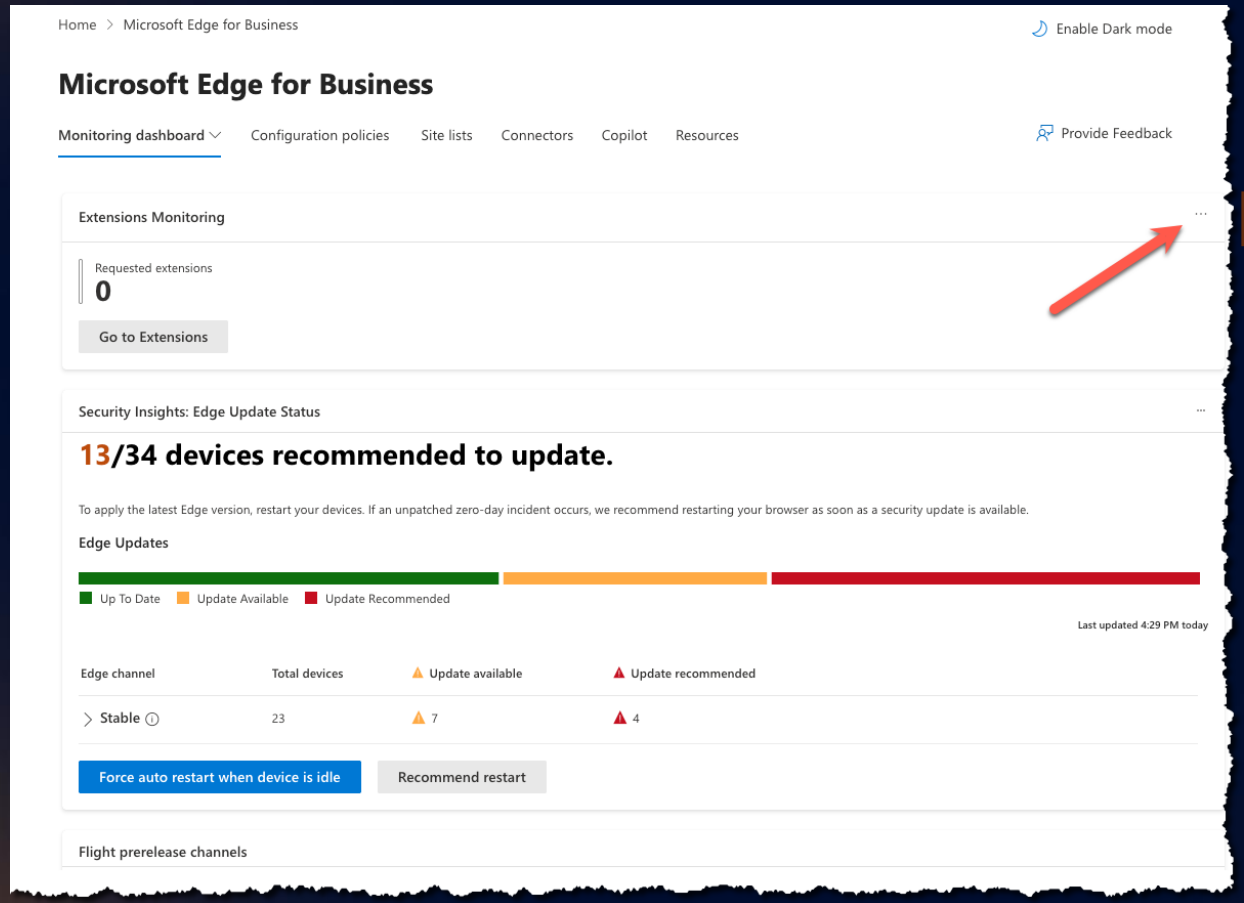
Monitoring (Targeted release)

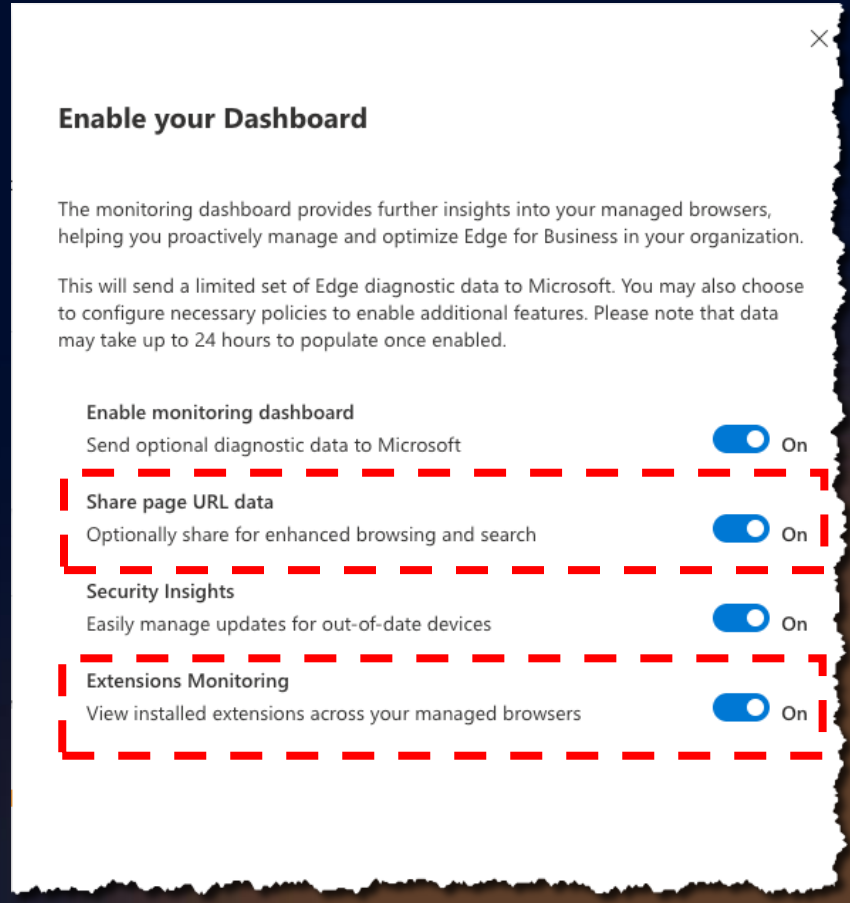






Privacy and Diagnostic





Demo

Edge extensions - security

- Extensions = any other software you run on your machine

Malwarebytes

Personal Business Pricing Partners Resources Help FREE DOWNLOAD

NEWS, THREATS

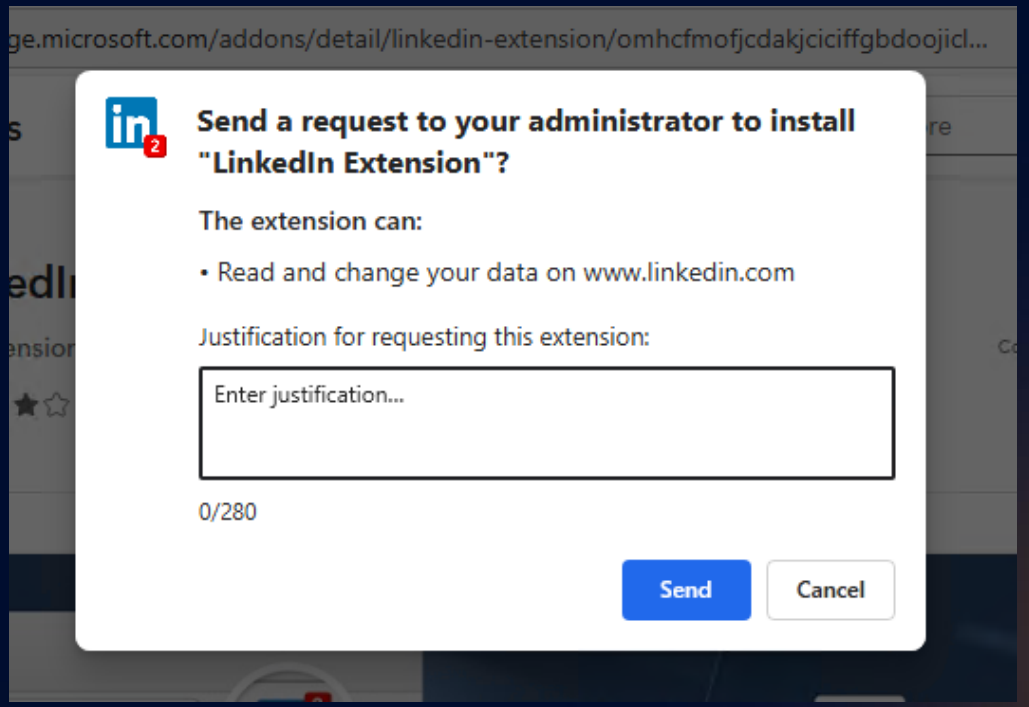
"Sleeper" browser extensions woke up as spyware on 4 million devices

by Pieter Arntz | December 2, 2025

https://www.malwarebytes.com/blog/news/2025/12/sleeper-browser-extensions-woke-up-as-spyware-on-4-million-devices

Request extensions

- Extensions are hard to manage, information security, GDPR…
- Instead of blocking and allowing we can allow the end-user to request an extension!



Extensions

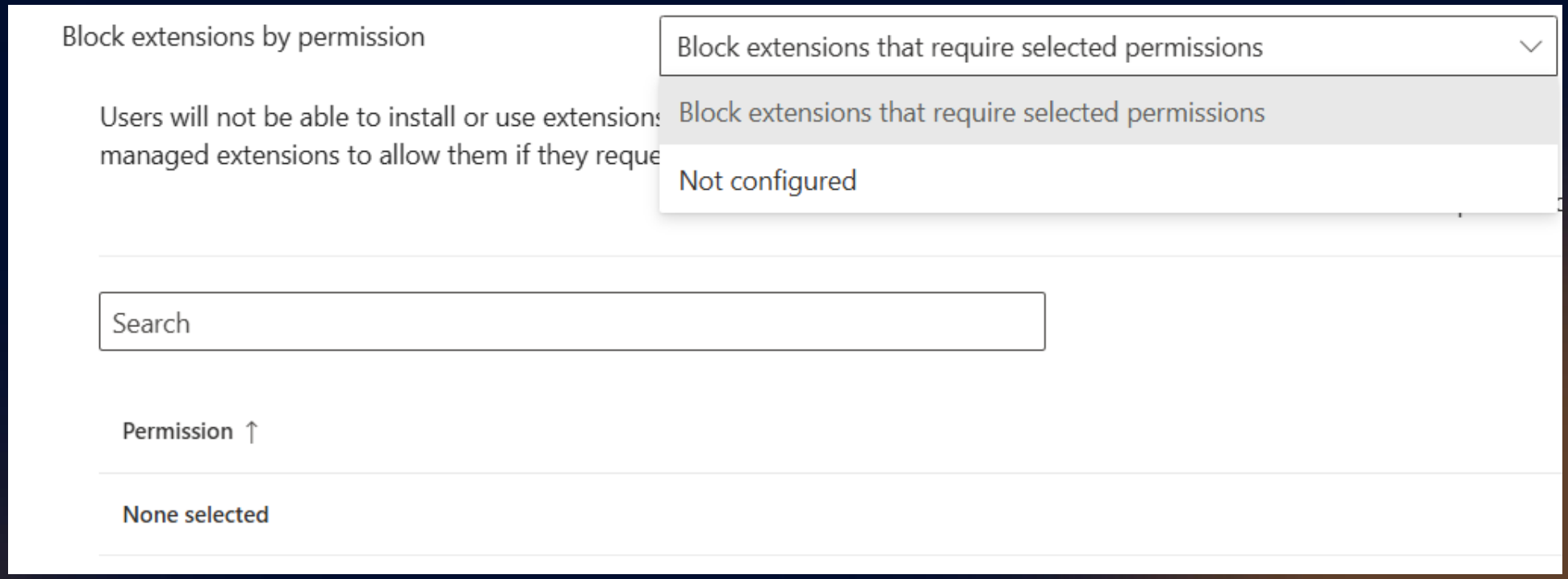
Requests

Manage request settings Refresh

	Name ↑	Number of requests	Last requested
☐	1Password – Password Manager	2	2025-07-07, 09:47:52
☐	AdBlock — block ads across the web	1	2025-07-07, 09:29:08
☐	Add to Microsoft To Do	1	2025-07-07, 09:28:08
☐	Microsoft 50th Anniversary – Celebration	1	2025-07-07, 09:28:35
☐	Microsoft Bing Homepage and Search Engine	1	2025-07-08, 14:39:00
☐	Microsoft Bing Search Engine	1	2025-07-07, 09:27:46
☐	Microsoft Editor: Spelling & Grammar Checker	1	2025-07-07, 09:47:14
☐	OneNote Web Clipper	1	2025-07-07, 09:28:20

Allow Extensions based on permissions

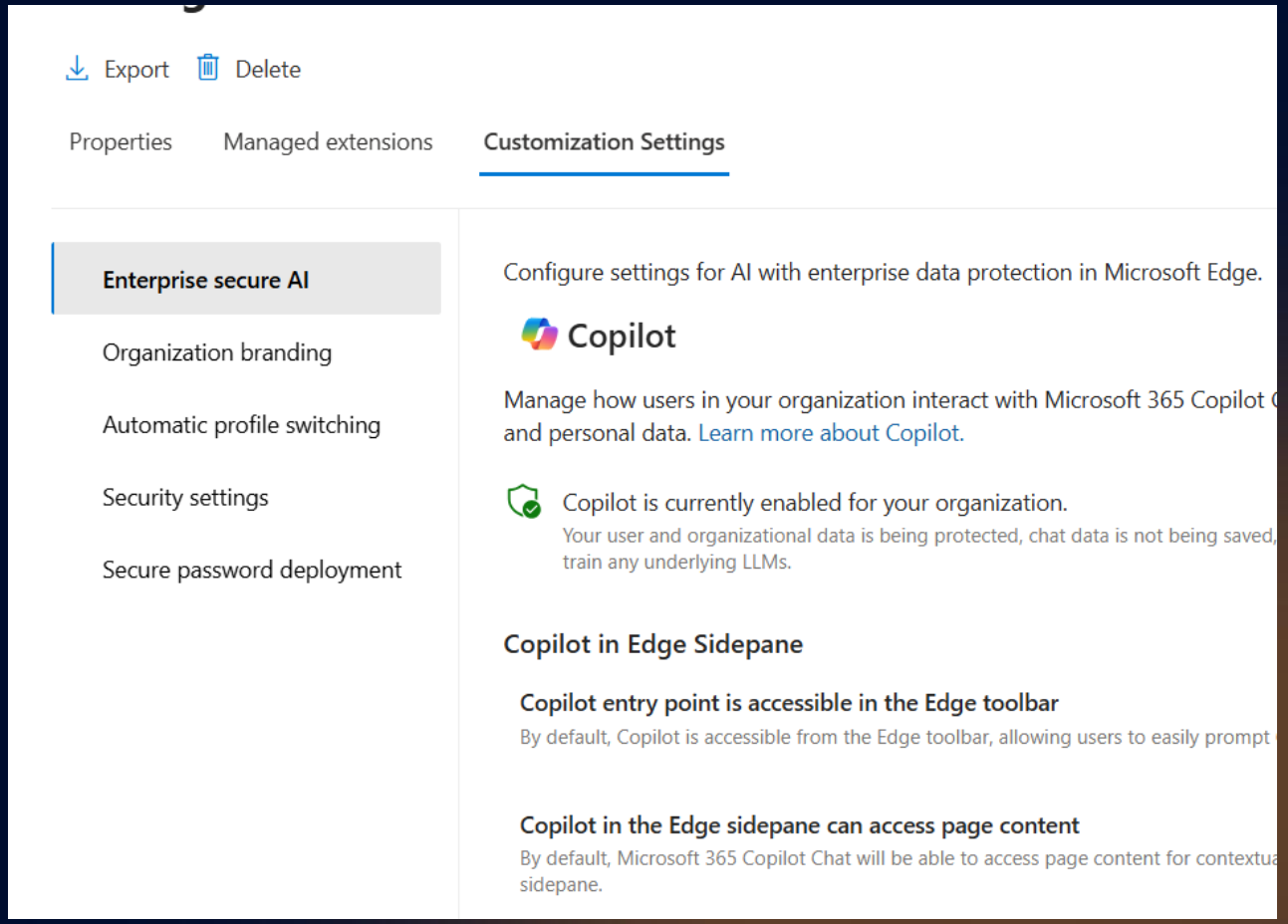
- Block extensions based on permissions
- Simplifies management to allow extensions based on permissions



Demo

Customization settings

- Enterprise secure AI
- Organisation branding
- Automatic profile switching
- Security settings
- Secure password deployment



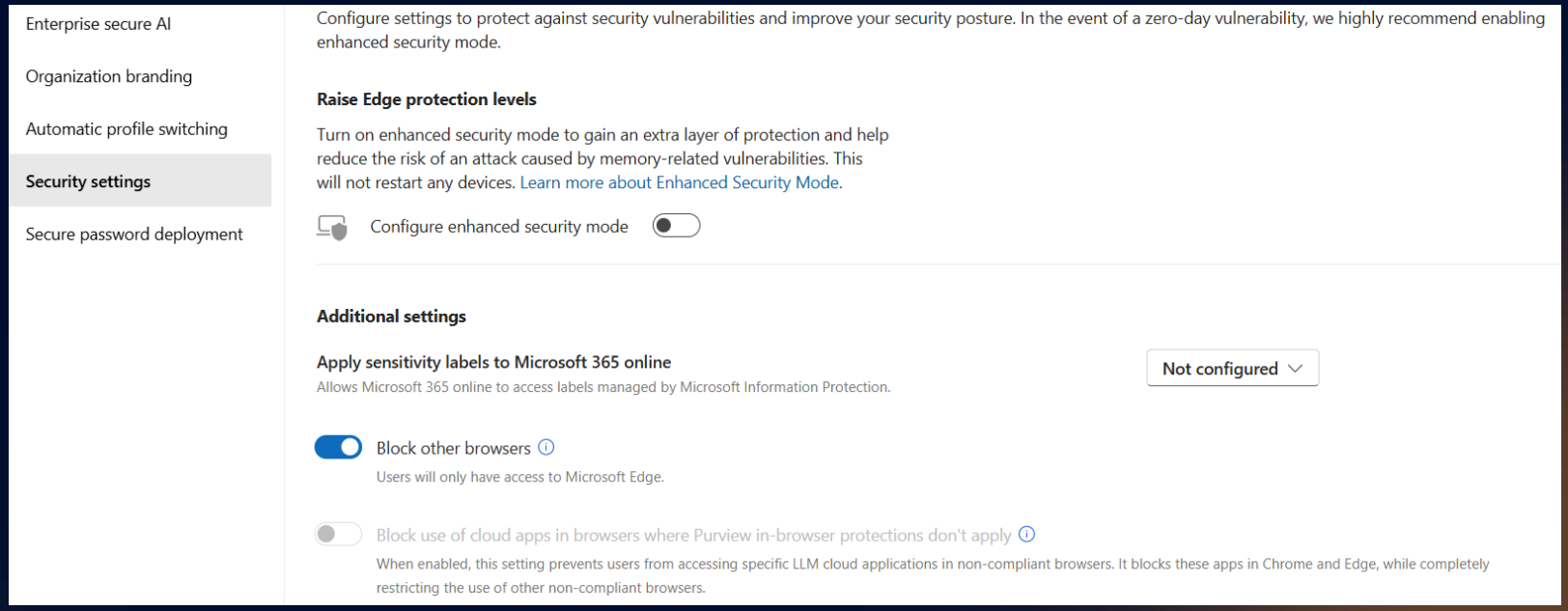
Enterprise Secure AI

https://bard.google.com, https://chat.openai.com, https://chatgpt.com,
https://chatgpt.es,
https://gemini.google.com, https://claude.ai
https://perplexity.ai, https://jasper.ai, https://you.com,
https://writesonic.com/chat, https://cohere.com/coral,
https://deepseek.com, https://deepseek.me

Demo

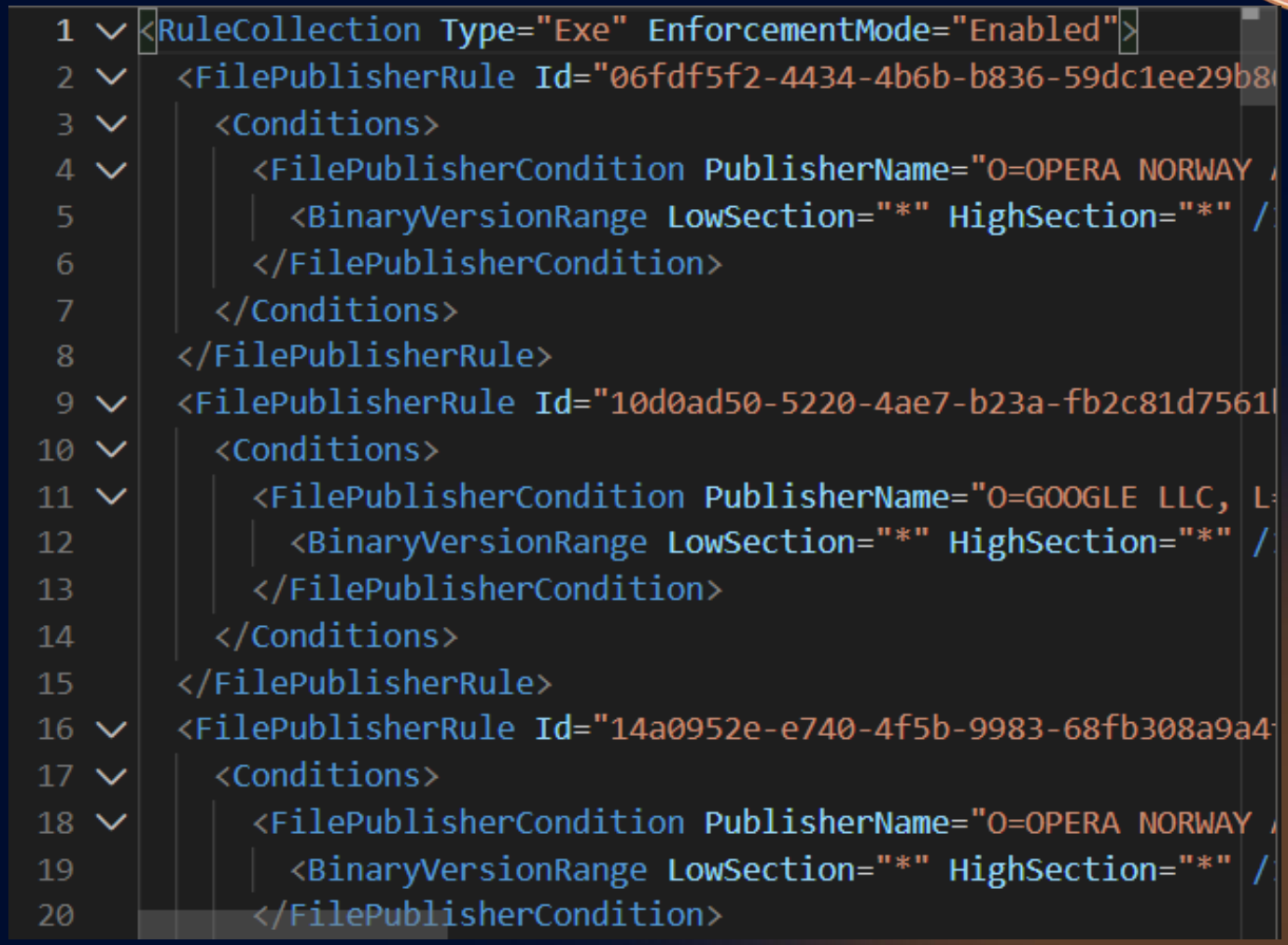
Block “other” Browsers

- Creates an AppLocker policy in Intune
- Both Executables and Store apps
- Requires Intune License



Blocked Browsers

- Opera
- Google Chrome
- FireFox
- Brave
- Vivaldi
- Tor Browser
- Puffin Secure Browser
- UC Browser
- Wave Browser
- DuckDuck GO



Demo

Security Baselines

- Reviewed for each version of Edge
- Current Security Baseline version = 139
- Version 140 – no new settings enforced
- Version 141 – no new settings enforced
- Version 142 – no new settings enforced
- Version 143 – no new settings enforced
- Version 144 – no new settings enforced
- Version 145 – no new settings enforced
- Version 146 – no new settings enforced
- Version 147 – no new settings enforced

Subscribe to changes – review them for every release of Edge

Microsoft Security Baselines Blog | Microsoft Community Hub

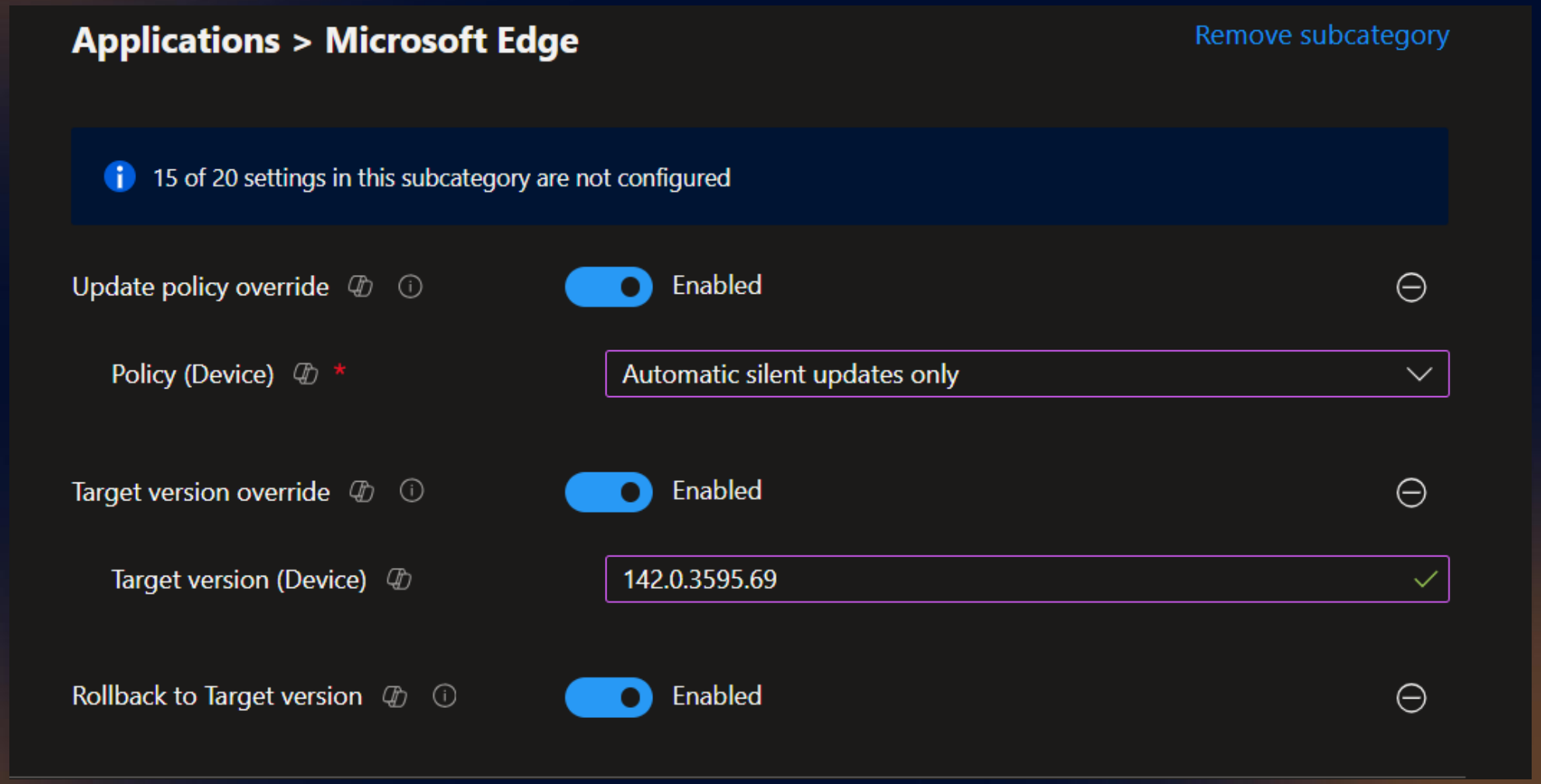
Rollback plan

- What happens if the CRM system no longe work in the latest release of Edge?
- Will take some days before Microsoft fix the issue.

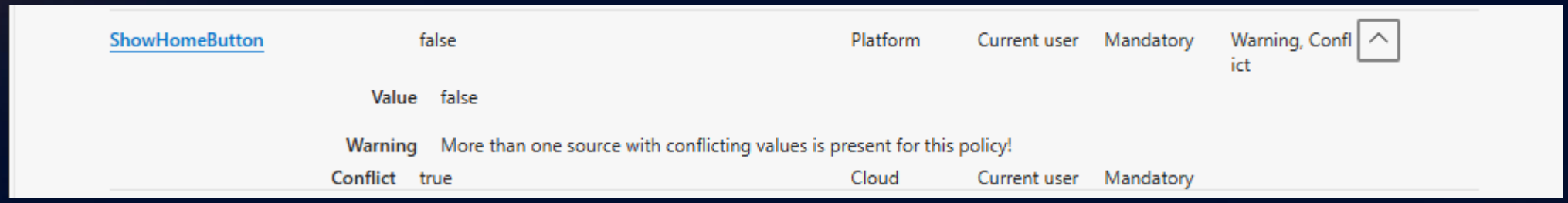
Solution:

- Deploy a secondary browser (Firefox?)
- Rollback Edge to a working version

Rollback settings



Edge Management Service vs. Intune

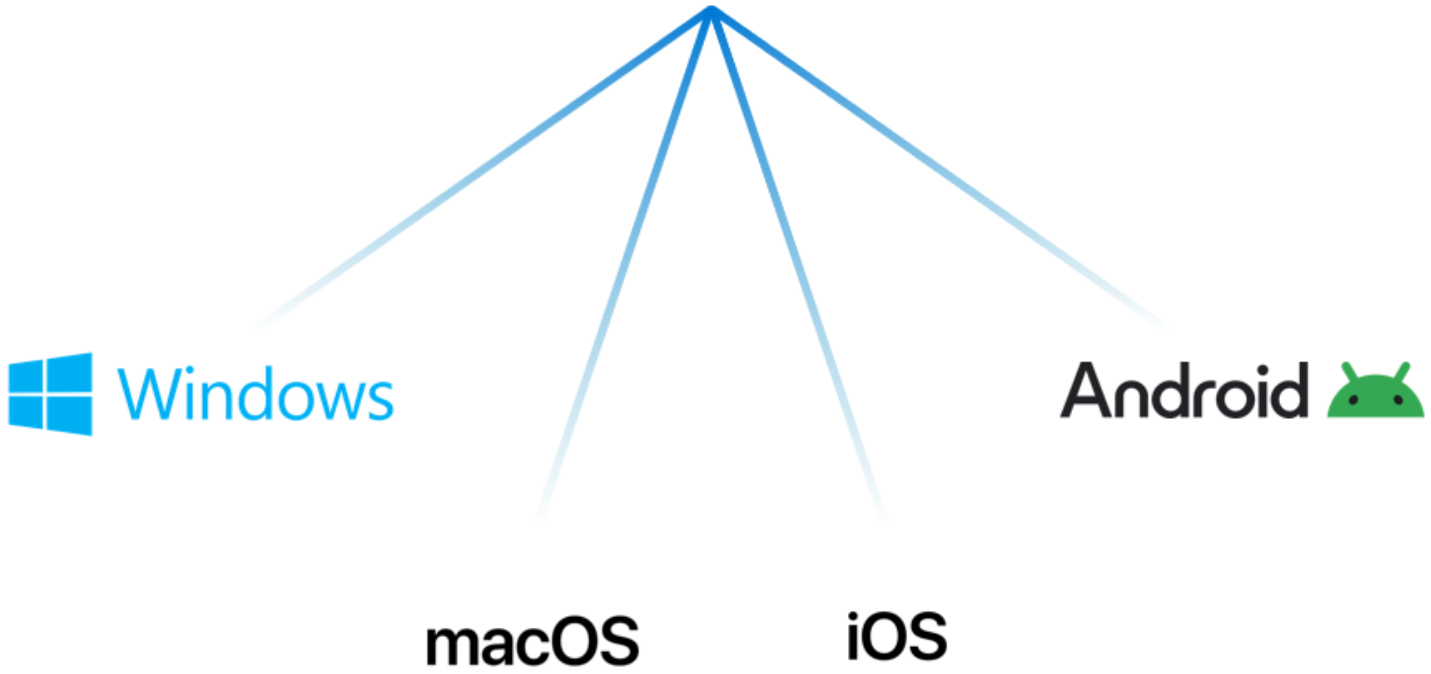


Two policies can be used to change this:

- EdgeManagementPolicyOverridesPlatformPolicy
- EdgeManagementUserPolicyOverridesCloudMachinePolicy

Multi platform support

Edge management service

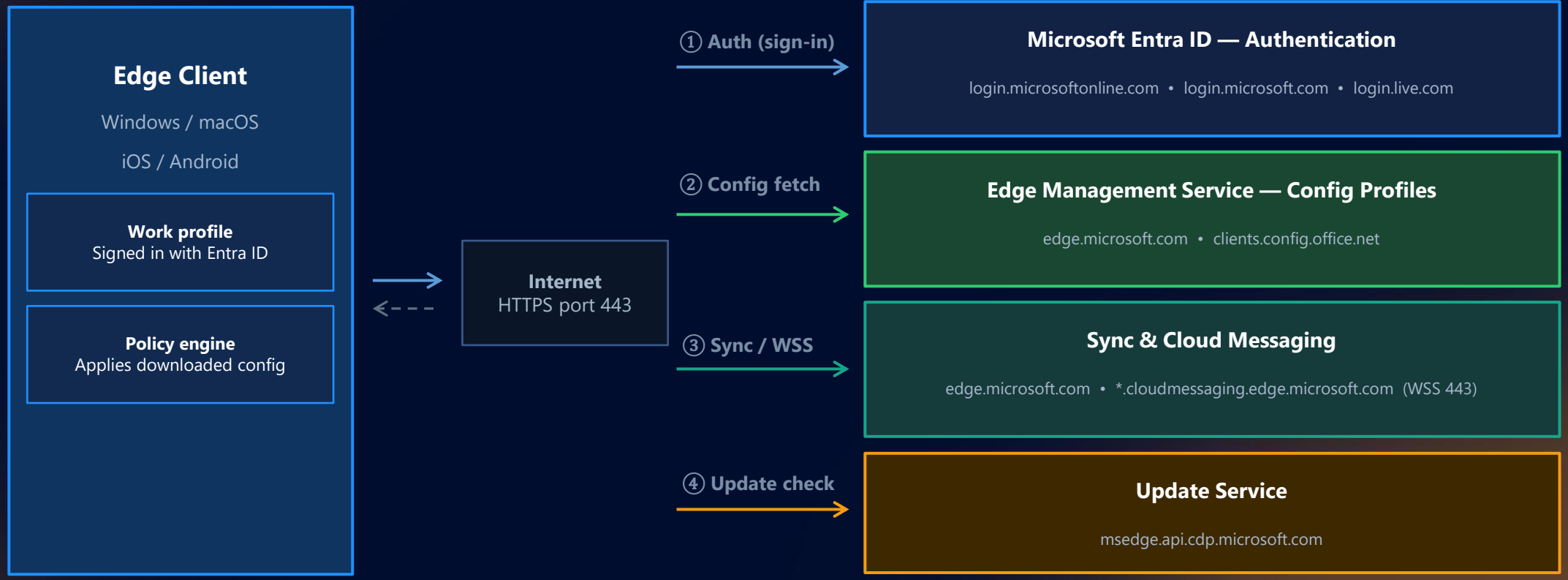


Policy sync - Intervals

- When a user signs into Microsoft Edge on a device for the first time
- Check for changes every 90 minutes.
- If there aren't any changes to the configuration policy since the last check, another check is made again in 24 hours.
- If there's an error, a check is made when the user opens Microsoft Edge.
- If Microsoft Edge isn't running when the next check is scheduled, then the check will be made the next time the user opens Microsoft Edge.

Edge Client → Edge Management Service

Traffic Flow & Required Endpoints



Authentication flow · Config / sync (HTTPS 443) · Update check · Response / return

Benefits

- macOS zero-day support for new settings
- One policy for all platforms
- Required to sign in for policies to apply except Windows
- Maybe not suitable for all settings depending on platform

Demo

B2B and BYOD support

Bring your own device (Windows)

- Use App Protection policy
- Require App Protection policy in Conditional Access
- Edge policies applies when user sign-in
  - We can control extensions
  - Security settings
  - Control access to AI in the Edge session
  - Security Baseline

B2B

When applying policies to B2B devices is more complex:

- Platform wins (device tenant)
- Force user login, blocks user from signing in to “guest” tenant = no policy
- Policies do apply when signing in

More complex!

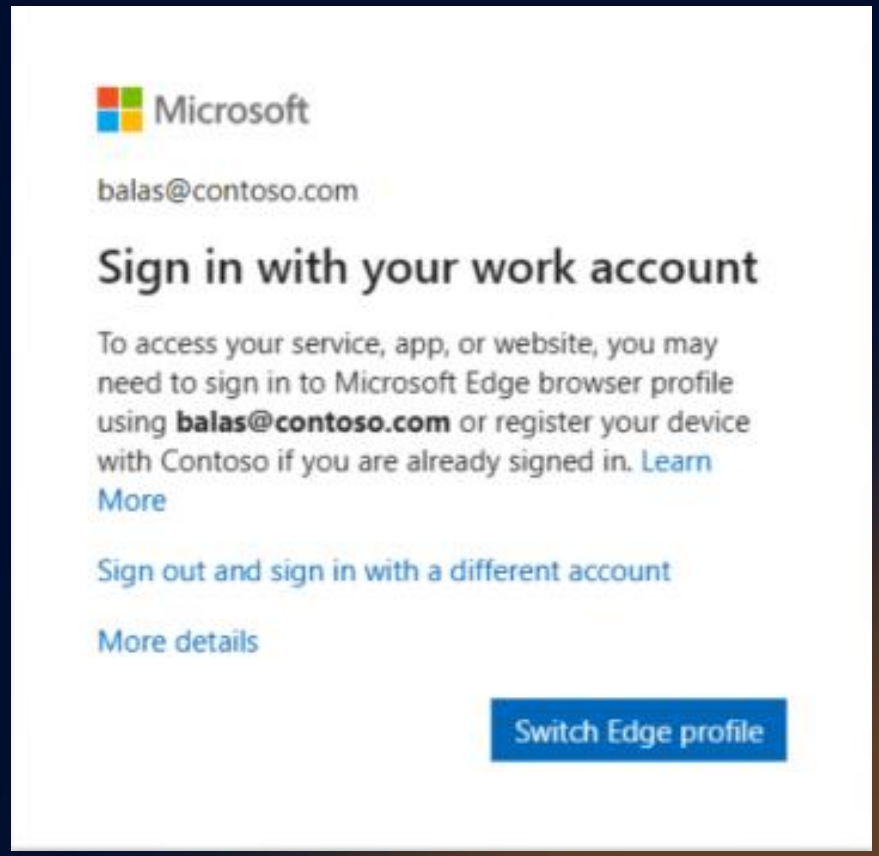
App protection policy for Edge

- Used to configure privacy settings in Edge for BYOD devices
- Privacy control:
  - Receive data from
  - Send org data to
  - Allow cut, copy, and paste
  - Printing org data
- Launch Control:
  - Version, offline control…

Step 2. Create App Protection Policies for Microsoft Edge for Business - Microsoft Intune | Microsoft Learn

Conditional Access – Force sign in

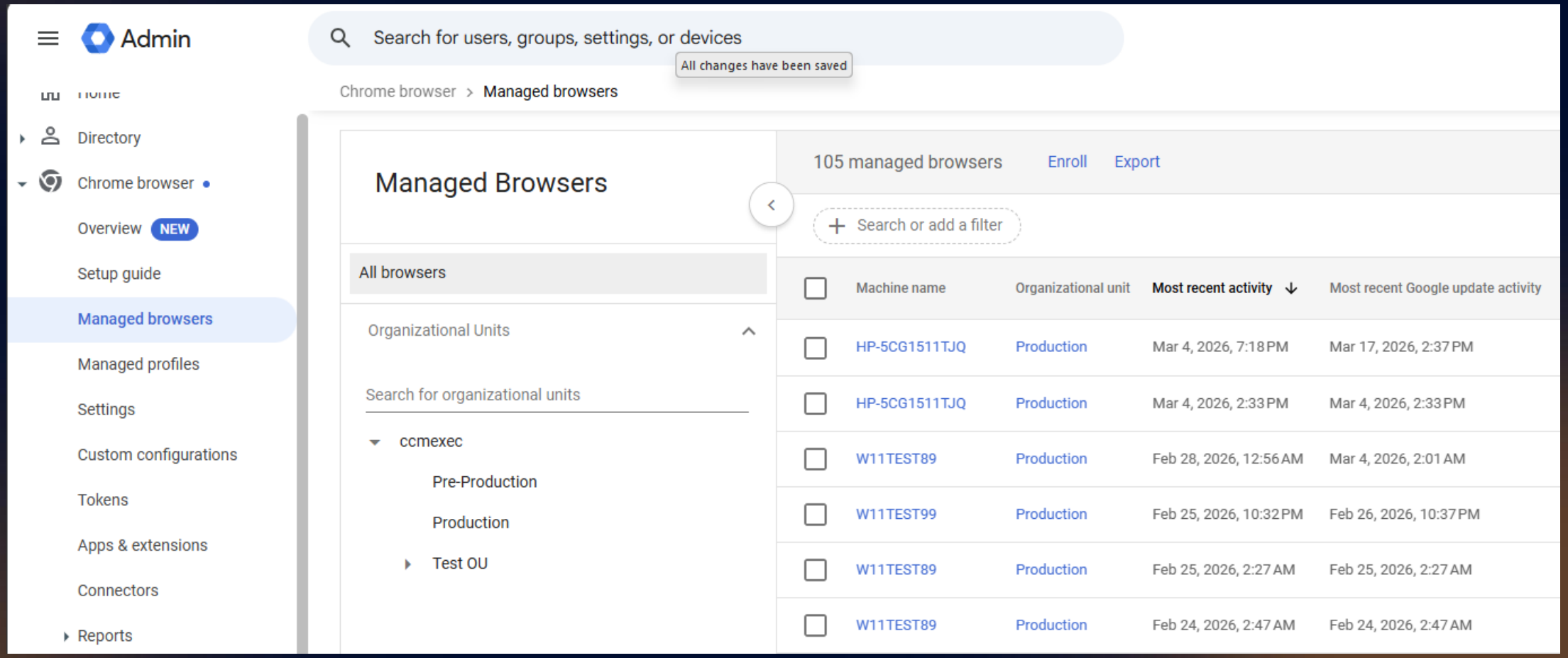
- For BYOD devices we can require App Protection using conditional access.
- If a user has not signed in Edge will receive a message that they must sign in.



Conditional Access - Require app protection policy for Windows - Microsoft Entra ID | Microsoft Learn

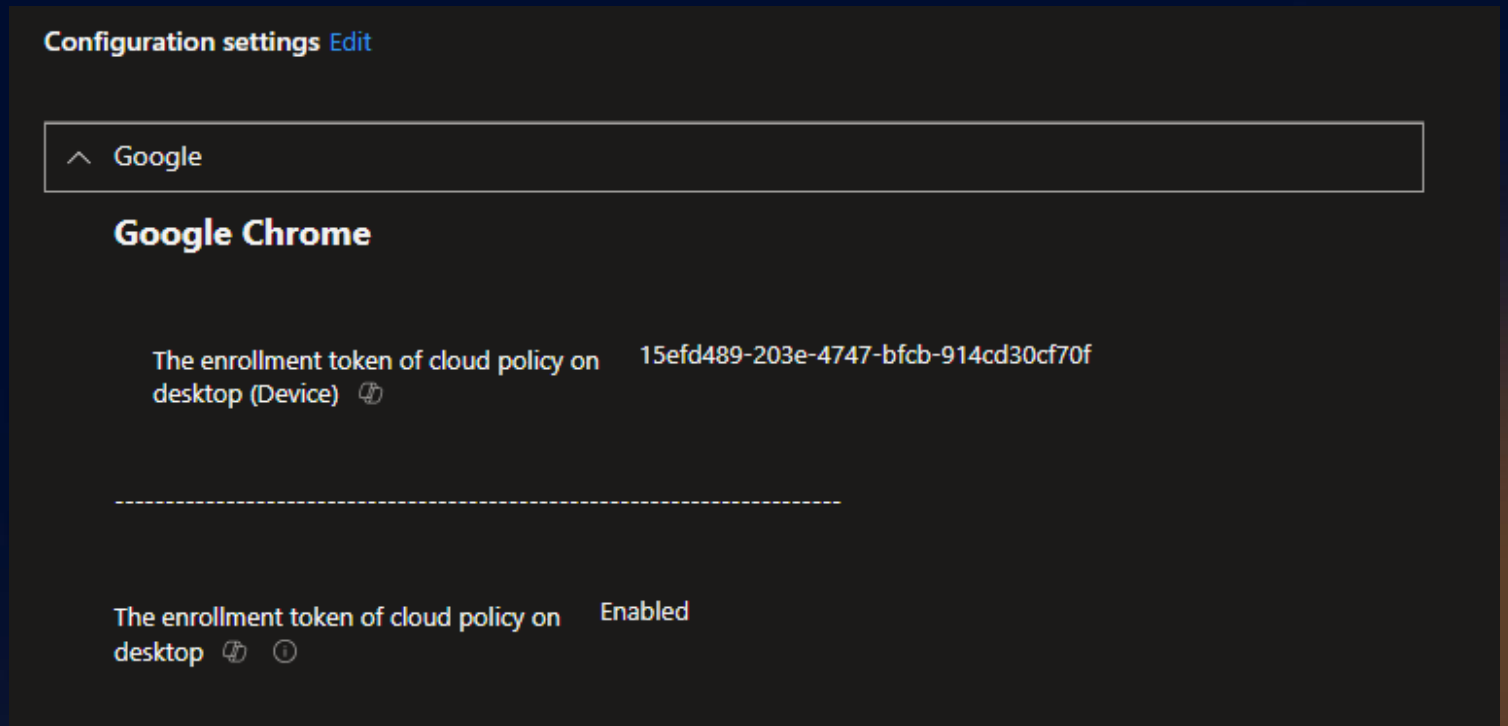
What about Google Chrome?!

Same functionality - free



Google Chrome Management

- Token per Organization unit
- Deploy token using Intune
- Configure per device



Chrome cloud management

Lessons learned

- Browser strategy is necessary – Allow/block
- Requires force user sign in in Edge if user target
- When requesting extensions we have no information about **WHO** requested it.
- No support for delegation/scope tags

- Time to move to a more secure and modern experience?

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!