



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, Apeno

Focus

Intune · Security · Windows · AI · Compliance

Blog, Hobbies and more

BBQ, Hiking

Sponsors



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

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

Edge Management Service



Windows

Mac

iOS/iPadOS

Android



Admin Portal



User Level



Device Level

Targeting

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



Deploy configuration profile

Select one or more existing configuration policies from Intune to deploy this profile to. Deploying this profile may overwrite any existing configuration for the EdgeManagementEnrollmentToken policy.

up policy, then copy the profile ID to use
mentToken policy.

Microsoft Edge

Remove category

Remove subcategory

Manageability

12 of 14 settings in this subcategory are not configured

Microsoft Edge management enrollment token (Device) `uc-alqX8yTpSrTpiE7XFYAQDa_REyKCqQK1eLrwIkVVnAAAAAAEWAAAF` ✓

Microsoft Edge management enrollment token Enabled

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)



Home > Microsoft Edge for Business Enable Dark mode

Microsoft Edge for Business

Monitoring dashboard | Configuration policies | Site lists | Connectors | Copilot | Resources

Extensions Monitoring

Requested extensions: **0**

[Go to Extensions](#)

Security Insights: Edge Update Status

13/34 devices recommended to update.

To apply the latest Edge version, restart your devices. If an unpatched zero-day incident occurs, we recommend restarting your browser as soon as possible.

Edge Updates

■ Up To Date ■ Update Available ■ Update Recommended

Edge channel	Total devices	Update available	Update recommended
> Stable ⓘ	23	7	4

[Force auto restart when device is idle](#) [Recommend restart](#)

Org settings

Services | Security & privacy | **Organization profile**

Name ↑	Description
Custom themes	Customize Microsoft Edge
Custom tiles for Apps	Add tiles that open when you click on the taskbar
Data location	See where Microsoft Edge stores your data
Help desk information	Streamline user support
Keyboard shortcuts	Perform many common tasks with a single keypress
Multitenant collaboration	Enable users in your organization to collaborate with users in other organizations
Organization information	Update your organization's name and logo
Release preferences	Choose how your organization gets new features and service updates
Send email notifications from your domain	Let Microsoft send you email notifications from your domain

Release preferences

Choose how your organization gets new features and service updates from Microsoft Edge.

[Learn more about release validation at Microsoft](#)

This setting doesn't affect how Microsoft 365 apps, such as Word and Excel, get new features and updates. To choose when Microsoft 365 apps get new features and updates, go to [Microsoft 365 installation options](#).

Standard release for everyone
Your entire organization gets updates when we release them from Microsoft Edge.

Targeted release for everyone
Your entire organization gets updates early.

Targeted release for select users
Pick people to receive updates early to preview them before they're available to everyone else.

Privacy and Diagnostic



Home > Microsoft Edge for Business Enable Dark mode

Microsoft Edge for Business

Monitoring dashboard Configuration policies Site lists Connectors Copilot Resources Provide Feedback

Extensions Monitoring

Requested extensions
0
[Go to Extensions](#)

Security Insights: Edge Update Status

13/34 devices recommended to update.

To apply the latest Edge version, restart your devices. If an unpatched zero-day incident occurs, we recommend restarting your browser as soon as a security update is available.

Edge Updates

Up To Date Update Available Update Recommended

Edge channel	Total devices	Update available	Update recommended
> Stable	23	7	4

[Force auto restart when device is idle](#) [Recommend restart](#)

Flight prerelease channels



Enable your Dashboard

The monitoring dashboard provides further insights into your managed browsers, helping you proactively manage and optimize Edge for Business in your organization.

This will send a limited set of Edge diagnostic data to Microsoft. You may also choose to configure necessary policies to enable additional features. Please note that data may take up to 24 hours to populate once enabled.

- Enable monitoring dashboard**
Send optional diagnostic data to Microsoft On
- Share page URL data**
Optionally share for enhanced browsing and search On
- Security Insights**
Easily manage updates for out-of-date devices On
- Extensions Monitoring**
View installed extensions across your managed browsers On



Demo



Edge extensions - security



- Extensions = any other software you run on your machine

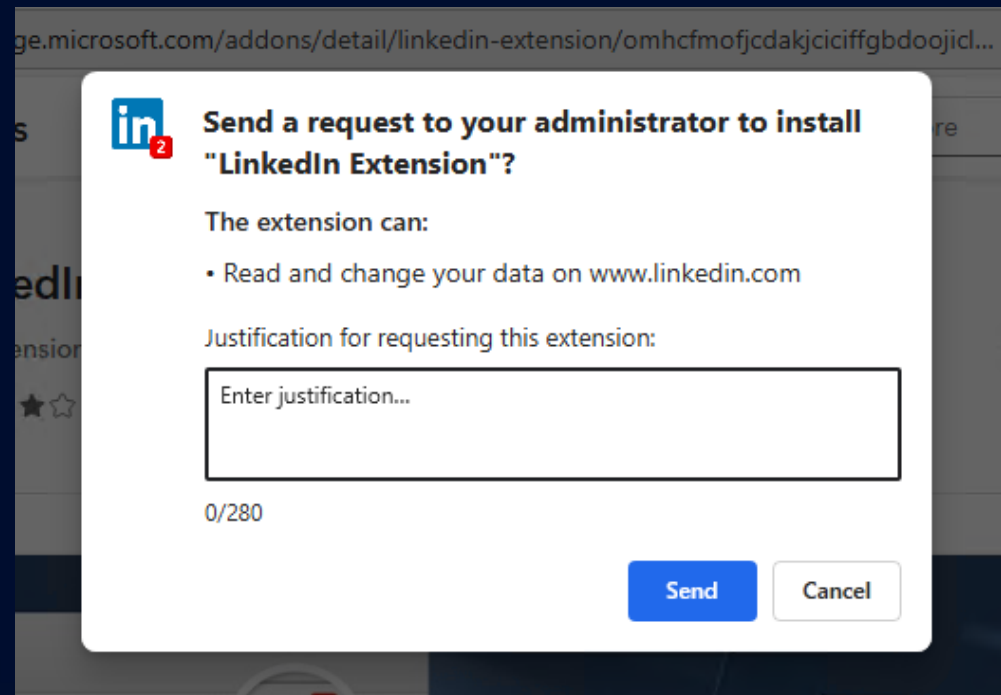
A screenshot of a Malwarebytes blog post. The header includes the Malwarebytes logo, navigation links for Personal, Business, Pricing, Partners, Resources, and Help, and a yellow 'FREE DOWNLOAD' button. The main content area features the text 'NEWS, THREATS' followed by the headline '"Sleeper" browser extensions woke up as spyware on 4 million devices' in large blue font. Below the headline are the logos for Google Chrome and Microsoft Edge. At the bottom left, it says '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
<input type="checkbox"/>	1Password – Password Manager	2	2025-07-07, 09:47:52
<input type="checkbox"/>	AdBlock — block ads across the web	1	2025-07-07, 09:29:08
<input type="checkbox"/>	Add to Microsoft To Do	1	2025-07-07, 09:28:08
<input type="checkbox"/>	Microsoft 50th Anniversary – Celebration	1	2025-07-07, 09:28:35
<input type="checkbox"/>	Microsoft Bing Homepage and Search Engine	1	2025-07-08, 14:39:00
<input type="checkbox"/>	Microsoft Bing Search Engine	1	2025-07-07, 09:27:46
<input type="checkbox"/>	Microsoft Editor: Spelling & Grammar Checker	1	2025-07-07, 09:47:14
<input type="checkbox"/>	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

Block extensions by permission

Block extensions that require selected permissions

Users will not be able to install or use extensions: managed extensions to allow them if they require

Block extensions that require selected permissions

Not configured

Search

Permission ↑

None selected



Demo



Customization settings

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



The screenshot shows the 'Customization Settings' page for 'Enterprise secure AI'. At the top, there are 'Export' and 'Delete' buttons. Below are tabs for 'Properties', 'Managed extensions', and 'Customization Settings'. The left sidebar lists settings: 'Enterprise secure AI' (selected), 'Organization branding', 'Automatic profile switching', 'Security settings', and 'Secure password deployment'. The main content area is titled 'Enterprise secure AI' and includes a description: 'Configure settings for AI with enterprise data protection in Microsoft Edge.' It features the Copilot logo and text: 'Manage how users in your organization interact with Microsoft 365 Copilot Chat and personal data. Learn more about Copilot.' A green checkmark icon indicates 'Copilot is currently enabled for your organization.' Below this, it states: 'Your user and organizational data is being protected, chat data is not being saved, and Copilot will not train any underlying LLMs.' Further down, there are sections for 'Copilot in Edge Sidepane' with sub-sections: 'Copilot entry point is accessible in the Edge toolbar' and 'Copilot in the Edge sidepane can access page content'.

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>

Other AI features

Manage additional AI features to protect your company and user data.

Users can access third-party LLM chatbots

By default, users will be able to access most major LLM-based chatbot sites other than Copilot.





Demo



Block "other" Browsers



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

Enterprise secure AI

Organization branding

Automatic profile switching


Security settings

Secure password deployment

Configure settings to protect against security vulnerabilities and improve your security posture. In the event of a zero-day vulnerability, we highly recommend enabling enhanced security mode.

Raise Edge protection levels

Turn on enhanced security mode to gain an extra layer of protection and help reduce the risk of an attack caused by memory-related vulnerabilities. This will not restart any devices. [Learn more about Enhanced Security Mode.](#)

 Configure enhanced security mode

Additional settings

Apply sensitivity labels to Microsoft 365 online Not configured ▾

Allows Microsoft 365 online to access labels managed by Microsoft Information Protection.

Block other browsers ⓘ

Users will only have access to Microsoft Edge.

Block use of cloud apps in browsers where Purview in-browser protections don't apply ⓘ

When enabled, this setting prevents users from accessing specific LLM cloud applications in non-compliant browsers. It blocks these apps in Chrome and Edge, while completely restricting the use of other non-compliant browsers.

Blocked Browsers



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

```
1 <RuleCollection Type="Exe" EnforcementMode="Enabled">
2   <FilePublisherRule Id="06fdf5f2-4434-4b6b-b836-59dc1ee29b80">
3     <Conditions>
4       <FilePublisherCondition PublisherName="O=OPERA NORWAY AS">
5         <BinaryVersionRange LowSection="*" HighSection="*" />
6       </FilePublisherCondition>
7     </Conditions>
8   </FilePublisherRule>
9   <FilePublisherRule Id="10d0ad50-5220-4ae7-b23a-fb2c81d75611">
10    <Conditions>
11      <FilePublisherCondition PublisherName="O=GOOGLE LLC, L">
12        <BinaryVersionRange LowSection="*" HighSection="*" />
13      </FilePublisherCondition>
14    </Conditions>
15  </FilePublisherRule>
16  <FilePublisherRule Id="14a0952e-e740-4f5b-9983-68fb308a9a41">
17    <Conditions>
18      <FilePublisherCondition PublisherName="O=OPERA NORWAY AS">
19        <BinaryVersionRange LowSection="*" HighSection="*" />
20      </FilePublisherCondition>
```



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 longer works in the latest release of Edge?
- Will take some days before Microsoft fixes the issue.

Solution:

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



Rollback settings



Applications > Microsoft Edge


[Remove subcategory](#)

i 15 of 20 settings in this subcategory are not configured

Update policy override  



Enabled



Policy (Device)  *


Automatic silent updates only



Target version override  



Enabled



Target version (Device) 

142.0.3595.69



Rollback to Target version  

Enabled



Edge Management Service vs. Intune



ShowHomeButton	false	Platform	Current user	Mandatory	Warning, Conflict	^
	Value false					
	Warning	More than one source with conflicting values is present for this policy!				
	Conflict true	Cloud	Current user	Mandatory		

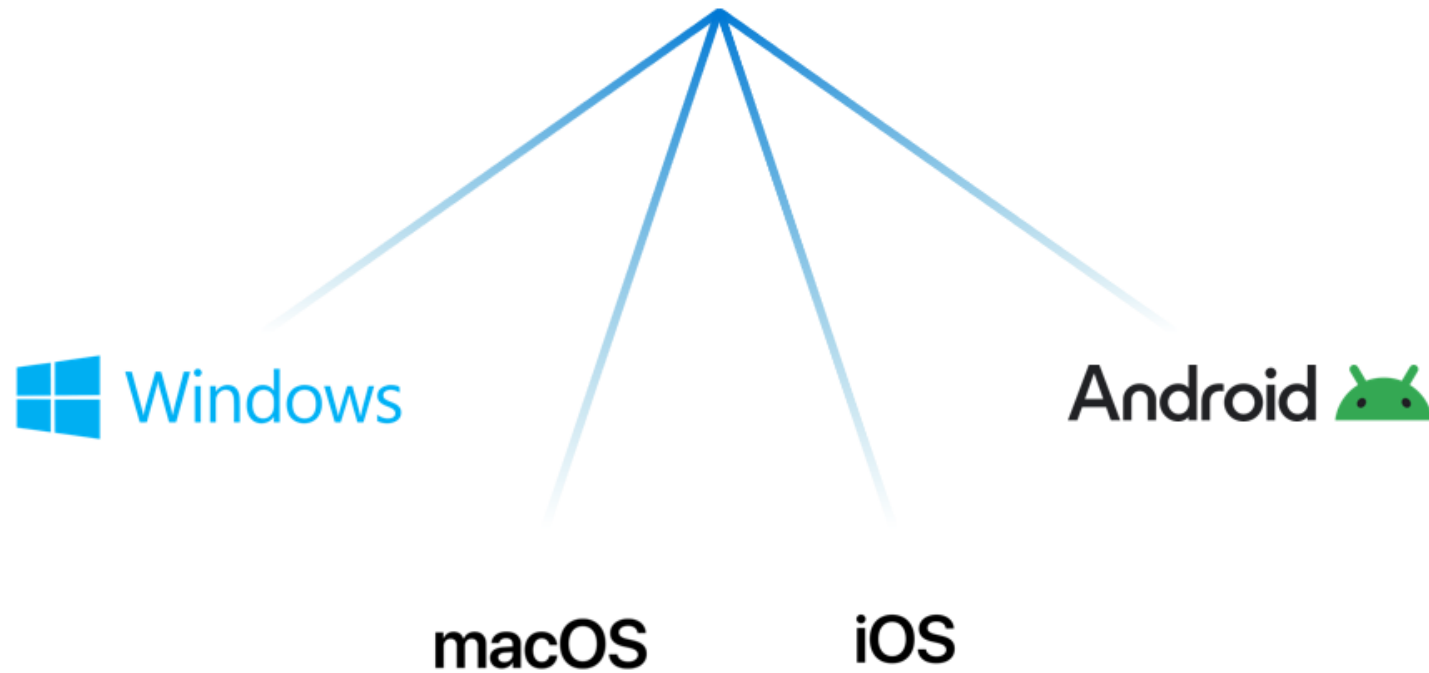
Two policies can be used to change this:

- EdgeManagementPolicyOverridesPlatformPolicy
- EdgeManagementUserPolicyOverridesCloudMachinePolicy



Multi platform support

Edge management service



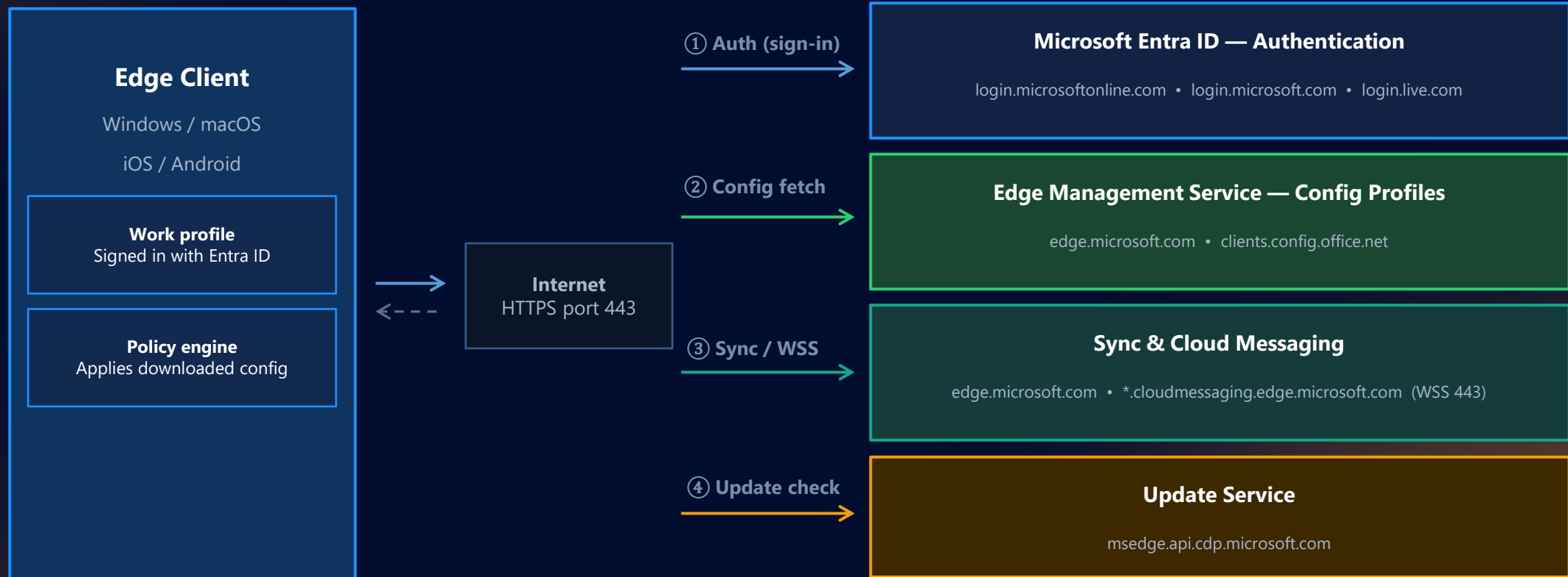
Policy sync - Intervals



- 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

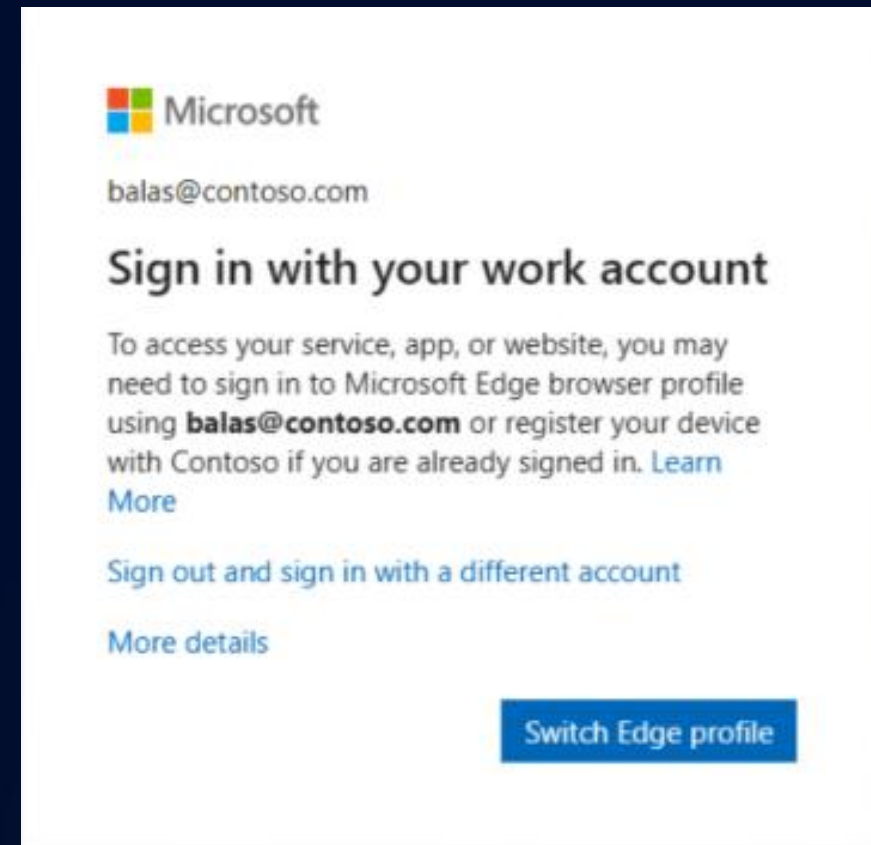


- Used to configure privacy settings in Edge for BYOD devices
- Privacy control:
 - Receive data from
 - Send org data to
 - Allow cut, copy, and paste
 - Printing org data
- Launch Control:
 - Version, offline control...

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.





What about Google Chrome?!

Same functionality - free



Admin

Search for users, groups, settings, or devices

All changes have been saved

Chrome browser > Managed browsers

Managed Browsers

105 managed browsers [Enroll](#) [Export](#)

<input type="checkbox"/>	Machine name	Organizational unit	Most recent activity ↓	Most recent Google update activity
<input type="checkbox"/>	HP-5CG1511TJQ	Production	Mar 4, 2026, 7:18 PM	Mar 17, 2026, 2:37 PM
<input type="checkbox"/>	HP-5CG1511TJQ	Production	Mar 4, 2026, 2:33 PM	Mar 4, 2026, 2:33 PM
<input type="checkbox"/>	W11TEST89	Production	Feb 28, 2026, 12:56 AM	Mar 4, 2026, 2:01 AM
<input type="checkbox"/>	W11TEST99	Production	Feb 25, 2026, 10:32 PM	Feb 26, 2026, 10:37 PM
<input type="checkbox"/>	W11TEST89	Production	Feb 25, 2026, 2:27 AM	Feb 25, 2026, 2:27 AM
<input type="checkbox"/>	W11TEST89	Production	Feb 24, 2026, 2:47 AM	Feb 24, 2026, 2:47 AM

Organizational Units

Search for organizational units

- ccmexec
 - Pre-Production
 - Production
 - Test OU

Google Chrome Management

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



Configuration settings [Edit](#)

^ Google

Google Chrome

The enrollment token of cloud policy on desktop (Device) [15efd489-203e-4747-bfcb-914cd30cf70f](#)

The enrollment token of cloud policy on desktop [Enabled](#)



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!