How to deploy Windows Autopatch with Microsoft Intune -By Robin Hobo -Published on Mar2,2023

Windows Autopatch is a service from Microsoft that automates the update process of Windows (both quality updates and feature updates), Microsoft 365 Apps for Enterprise (aka Office apps), the Microsoft Edge browser and Microsoft Teams. Once the service is enabled in your tenant and devices are onboarded successful you don't need to worry about updates of the supported products anymore. Microsoft will take care of it.

Prerequisites of Windows Autopatch

- Windows 10/11 Enterprise E3 or higher licenses
- Azure AD P1 or higher licenses
- Microsoft Intune licenses
- Windows build 1809 or higher
- Users must exist in Azure AD (synced or cloud-only)
- Devices needs to be under management of Microsoft Intune or Configuration Manager Co-managed

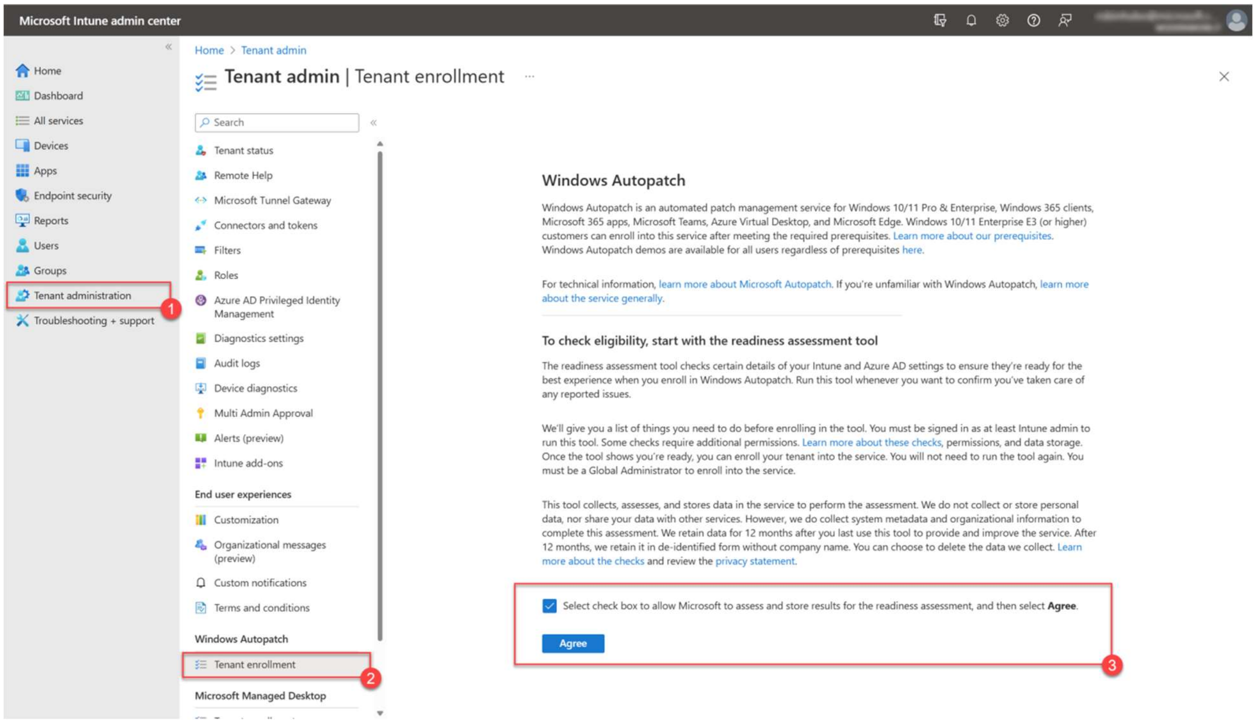
Table of content

The following steps will step-by-step described in this blog.

1. Enable Windows Autopatch
2. Onboard devices to Windows Autopatch
3. Managing Windows Autopatch

1 – Enable Windows Autopatch

For the next steps, navigate to the Microsoft Intune admin center.



Windows Autopatch

Windows Autopatch is an automated patch management service for Windows 10/11 Pro & Enterprise, Windows 365 clients, Microsoft 365 apps, Microsoft Teams, Azure Virtual Desktop, and Microsoft Edge. Windows 10/11 Enterprise E3 (or higher) customers can enroll into this service after meeting the required prerequisites. Learn more about our prerequisites. Windows Autopatch demos are available for all users regardless of prerequisites here.

For technical information, learn more about Microsoft Autopatch. If you're unfamiliar with Windows Autopatch, learn more about the service generally.

To check eligibility, start with the readiness assessment tool

The readiness assessment tool checks certain details of your Intune and Azure AD settings to ensure they're ready for the best experience when you enroll in Windows Autopatch. Run this tool whenever you want to confirm you've taken care of any reported issues.

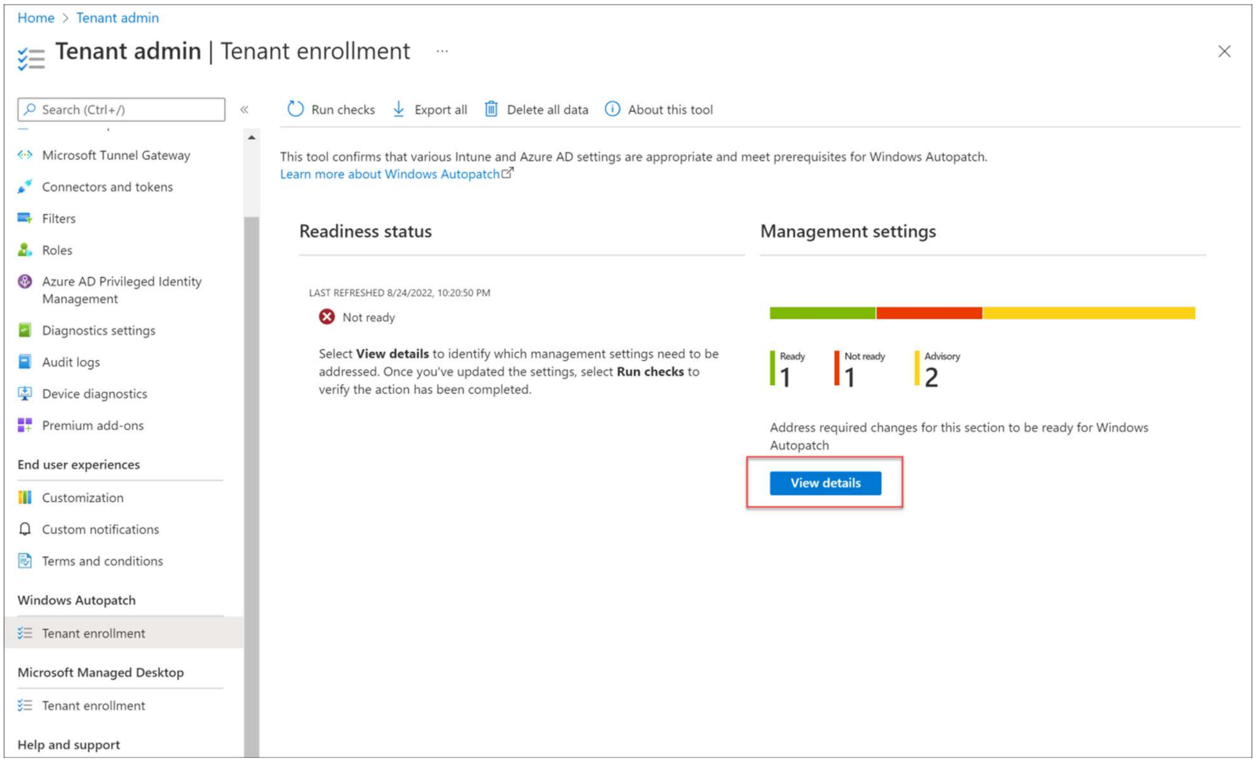
We'll give you a list of things you need to do before enrolling in the tool. You must be signed in as at least Intune admin to run this tool. Some checks require additional permissions. Learn more about these checks, permissions, and data storage. Once the tool shows you're ready, you can enroll your tenant into the service. You will not need to run the tool again. You must be a Global Administrator to enroll into the service.

This tool collects, assesses, and stores data in the service to perform the assessment. We do not collect or store personal data, nor share your data with other services. However, we do collect system metadata and organizational information to complete this assessment. We retain data for 12 months after you last use this tool to provide and improve the service. After 12 months, we retain it in de-identified form without company name. You can choose to delete the data we collect. Learn more about the checks and review the privacy statement.

☑ Select check box to allow Microsoft to assess and store results for the readiness assessment, and then select **Agree**.

Agree

Navigate to **Tenant administration > Tenant enrollment**. Select the checkbox and click **Agree**.



This tool confirms that various Intune and Azure AD settings are appropriate and meet prerequisites for Windows Autopatch. Learn more about Windows Autopatch

Readiness status

LAST REFRESHED 8/24/2022, 10:20:50 PM

Not ready

Select **View details** to identify which management settings need to be addressed. Once you've updated the settings, select **Run checks** to verify the action has been completed.

Management settings

Address required changes for this section to be ready for Windows Autopatch

First we need to run the **Readiness assessment tool** to see if we can enable the service and we met all the requirements. The results of the test can have one of the following status.

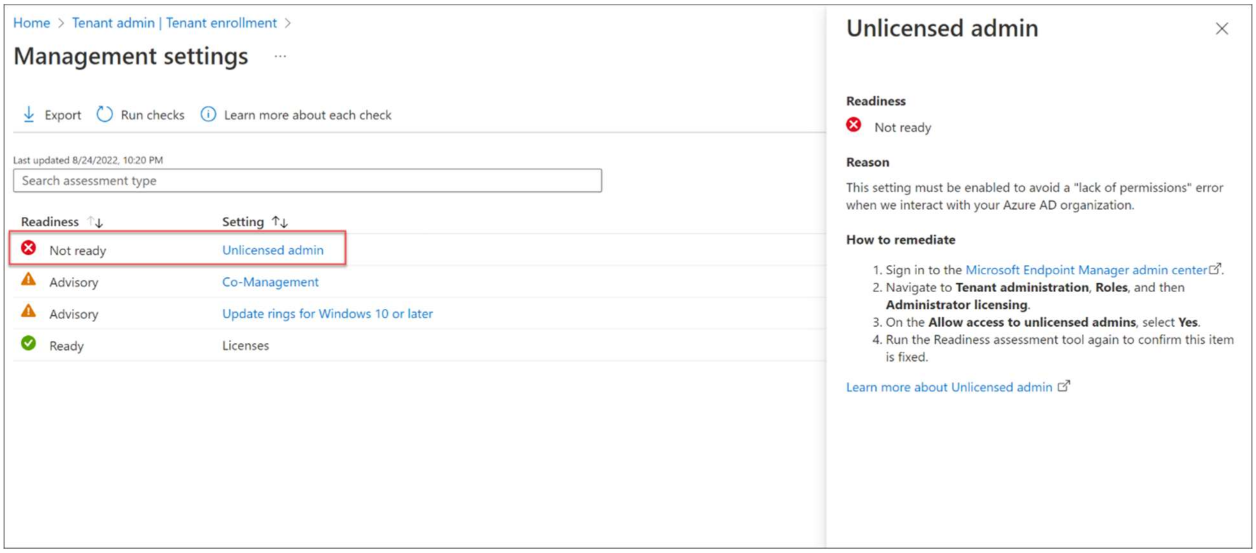
Ready – Ready to go, no actions are required

Advisory – An advice to get the best experience once the service is up and running, not a requirement and so, not a blocker

Not ready – A show stopper that needs to be fixed before you can continue

Error – Mostly related to insufficient permissions to run this task

In my case I have some advisory and not ready points, lets discuss them from top to bottom. Click **View details**.


Home > Tenant admin | Tenant enrollment >
Management settings ...
Export
Run checks
Learn more about each check

Last updated 8/24/2022, 10:20 PM

Readiness ↑↓	Setting ↑↓
Not ready	Unlicensed admin
Advisory	Co-Management
Advisory	Update rings for Windows 10 or later
Ready	Licenses

Unlicensed admin

Readiness

Not ready

Reason

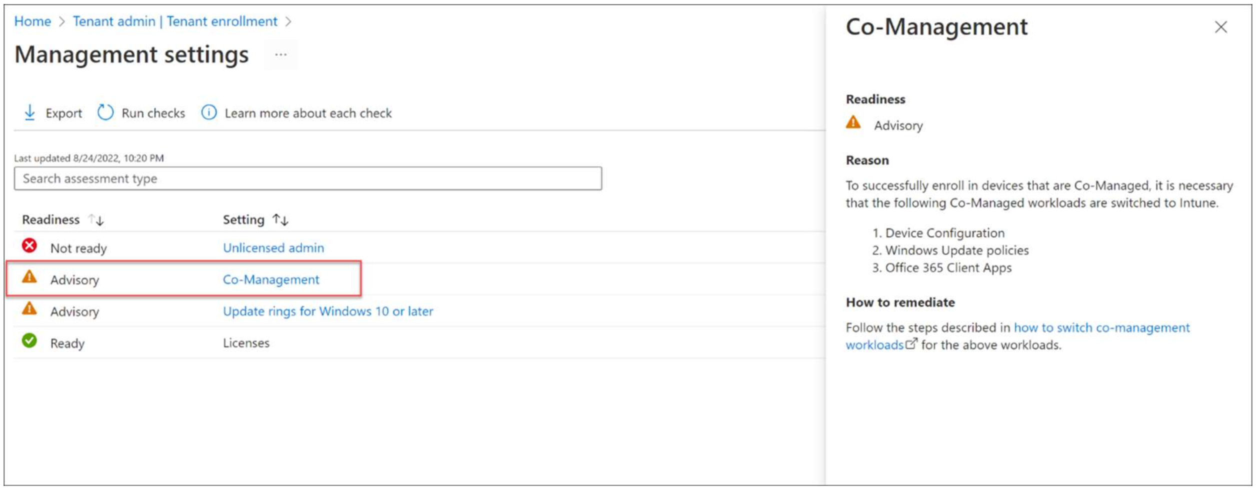
This setting must be enabled to avoid a "lack of permissions" error when we interact with your Azure AD organization.

How to remediate

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Navigate to **Tenant administration**, **Roles**, and then **Administrator licensing**.
3. On the **Allow access to unlicensed admins**, select **Yes**.
4. Run the Readiness assessment tool again to confirm this item is fixed.

Learn more about Unlicensed admin

The first point is about **Unlicensed admin**, this is a requirement for this service and I did not enable this feature yet. When clicking on the setting on the left, the instructions about the required steps that needs to be made are displayed on the right.



Home > Tenant admin | Tenant enrollment >

Management settings ···

Last updated 8/24/2022, 10:20 PM

Search assessment type

Readiness ↑↓	Setting ↑↓
✖ Not ready	Unlicensed admin
⚠ Advisory	Co-Management
⚠ Advisory	Update rings for Windows 10 or later
✓ Ready	Licenses

Co-Management

Readiness

⚠ Advisory

Reason

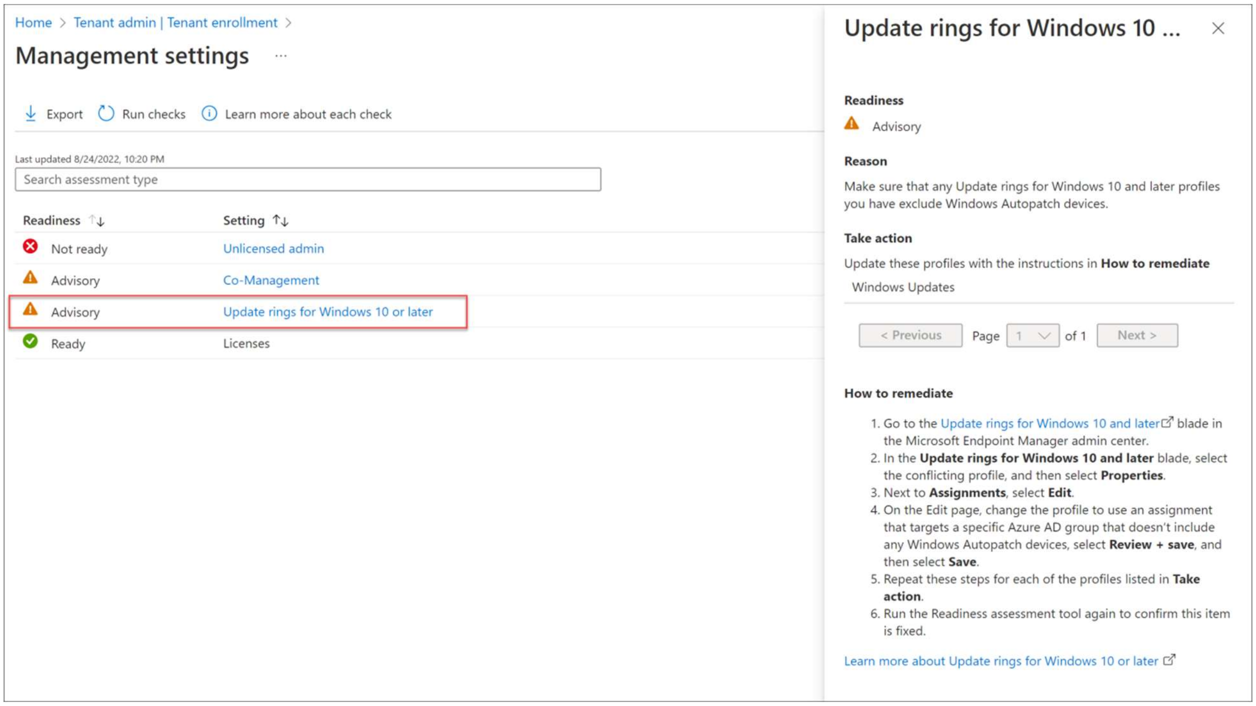
To successfully enroll in devices that are Co-Managed, it is necessary that the following Co-Managed workloads are switched to Intune.

1. Device Configuration
2. Windows Update policies
3. Office 365 Client Apps

How to remediate

Follow the steps described in how to switch co-management workloads for the above workloads.

Second point is an Advisory about co-management configuration. I did not setup co-management in my environment so I will ignore this one.



Home > Tenant admin | Tenant enrollment >

Management settings ···

Last updated 8/24/2022, 10:20 PM

Search assessment type

Readiness ↑↓	Setting ↑↓
✖ Not ready	Unlicensed admin
⚠ Advisory	Co-Management
⚠ Advisory	Update rings for Windows 10 or later
✓ Ready	Licenses

Update rings for Windows 10 ...

Readiness

⚠ Advisory

Reason

Make sure that any Update rings for Windows 10 and later profiles you have exclude Windows Autopatch devices.

Take action

Update these profiles with the instructions in **How to remediate**

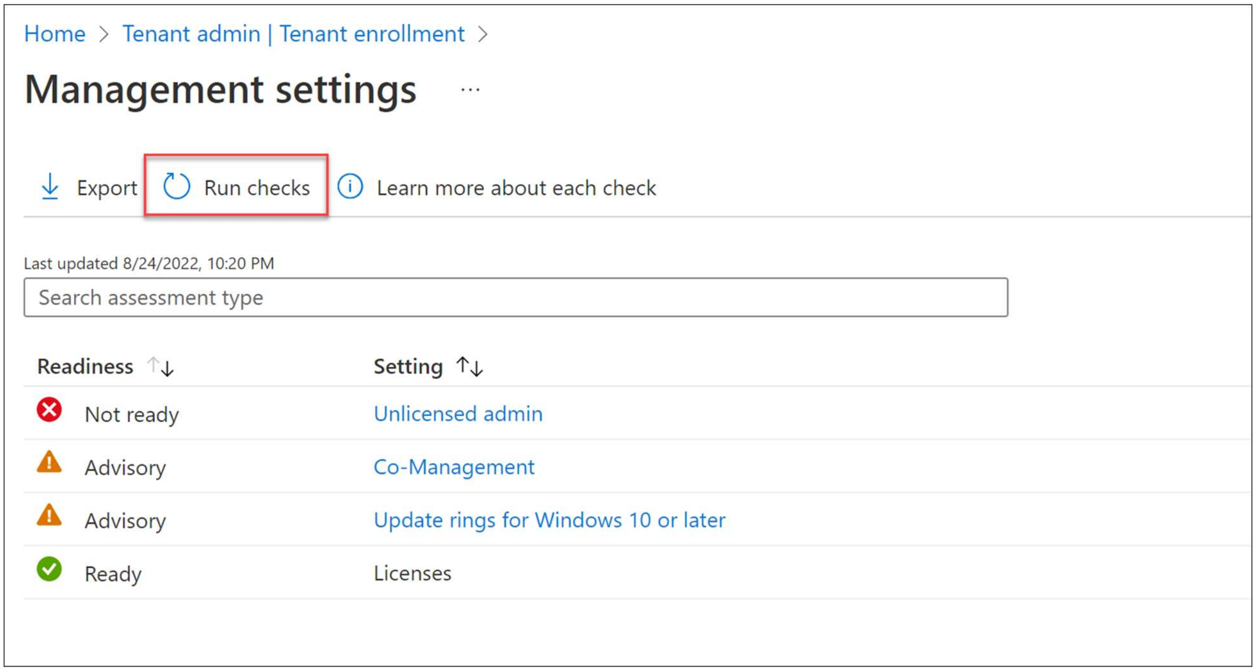
Windows Updates

How to remediate

1. Go to the Update rings for Windows 10 and later blade in the Microsoft Endpoint Manager admin center.
2. In the **Update rings for Windows 10 and later** blade, select the conflicting profile, and then select **Properties**.
3. Next to **Assignments**, select **Edit**.
4. On the Edit page, change the profile to use an assignment that targets a specific Azure AD group that doesn't include any Windows Autopatch devices, select **Review + save**, and then select **Save**.
5. Repeat these steps for each of the profiles listed in **Take action**.
6. Run the Readiness assessment tool again to confirm this item is fixed.

Learn more about Update rings for Windows 10 or later

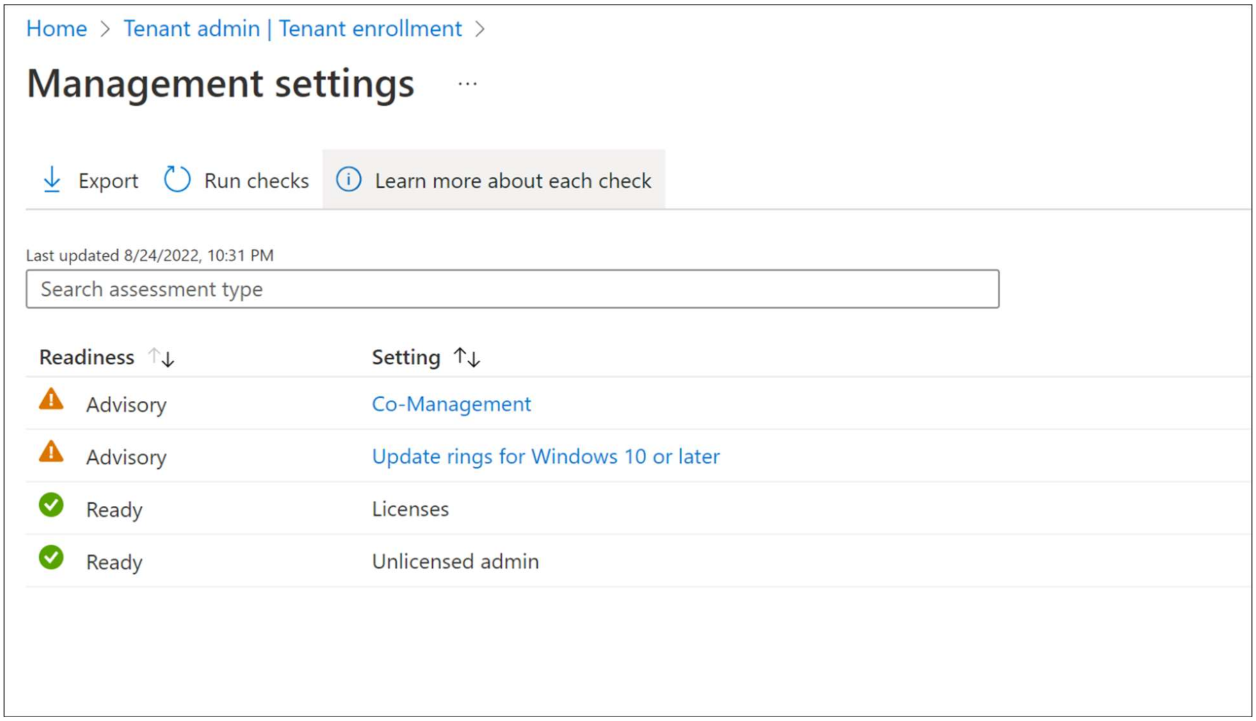
Next point is an important one. I have setup Update policies for Windows 10 and later devices. These settings can conflict with the settings of Windows Autopatch. Make sure that you exclude Autopatch devices from current Windows Update rings policies. See instructions on the right for more information in the screenshot.


Home > Tenant admin | Tenant enrollment >
Management settings ...
Export
Run checks
Learn more about each check
Search assessment type

Last updated 8/24/2022, 10:20 PM

Readiness ↑↓	Setting ↑↓
⊗ Not ready	Unlicensed admin
⚠ Advisory	Co-Management
⚠ Advisory	Update rings for Windows 10 or later
✓ Ready	Licenses

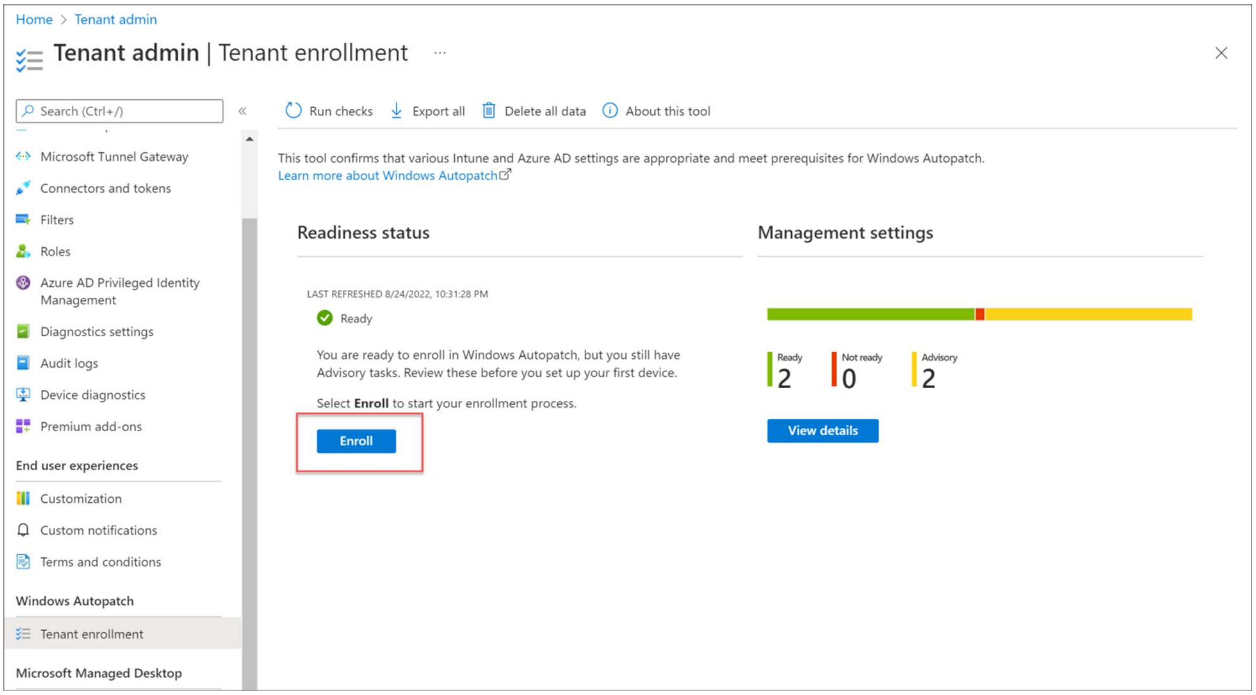
After changing the required and advised settings, click **Run check**


Home > Tenant admin | Tenant enrollment >
Management settings ...
Export
Run checks
Learn more about each check
Search assessment type

Last updated 8/24/2022, 10:31 PM

Readiness ↑↓	Setting ↑↓
⚠ Advisory	Co-Management
⚠ Advisory	Update rings for Windows 10 or later
✓ Ready	Licenses
✓ Ready	Unlicensed admin

We are now ready to go.



This tool confirms that various Intune and Azure AD settings are appropriate and meet prerequisites for Windows Autopatch.
Learn more about Windows Autopatch

Readiness status

LAST REFRESHED 8/24/2022, 10:31:28 PM

Ready

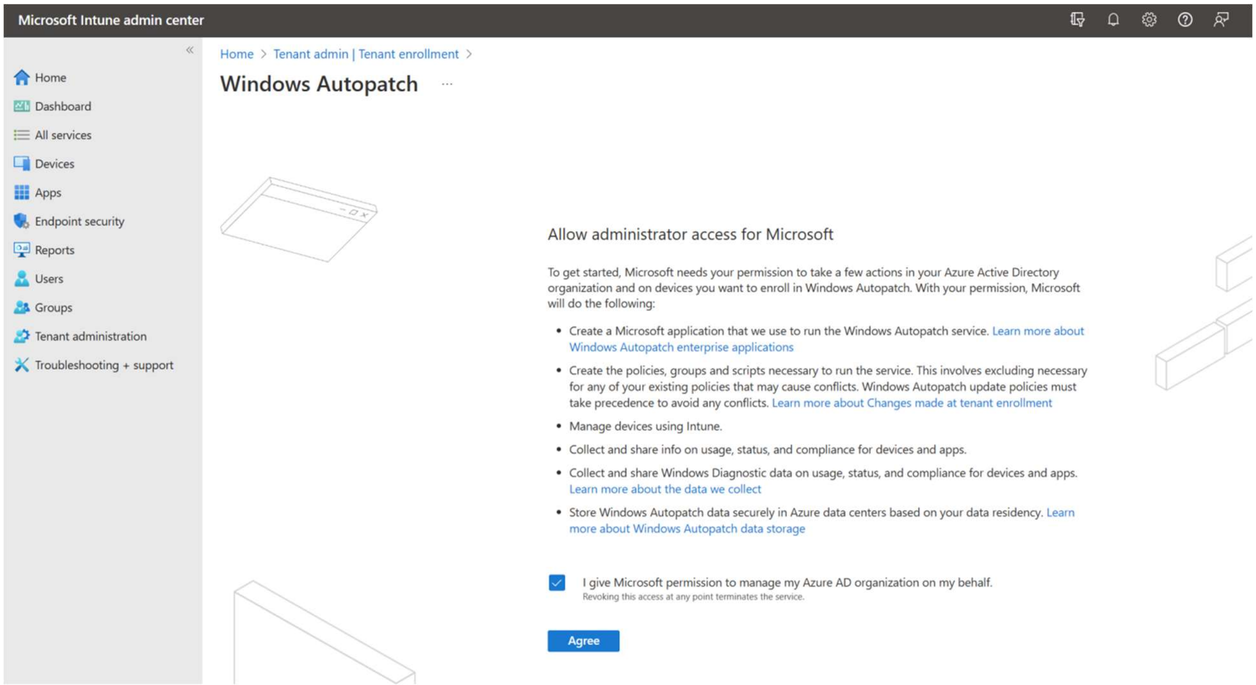
You are ready to enroll in Windows Autopatch, but you still have Advisory tasks. Review these before you set up your first device.

Select **Enroll** to start your enrollment process.

Management settings

Ready	Not ready	Advisory
2	0	2

Click **Enroll**



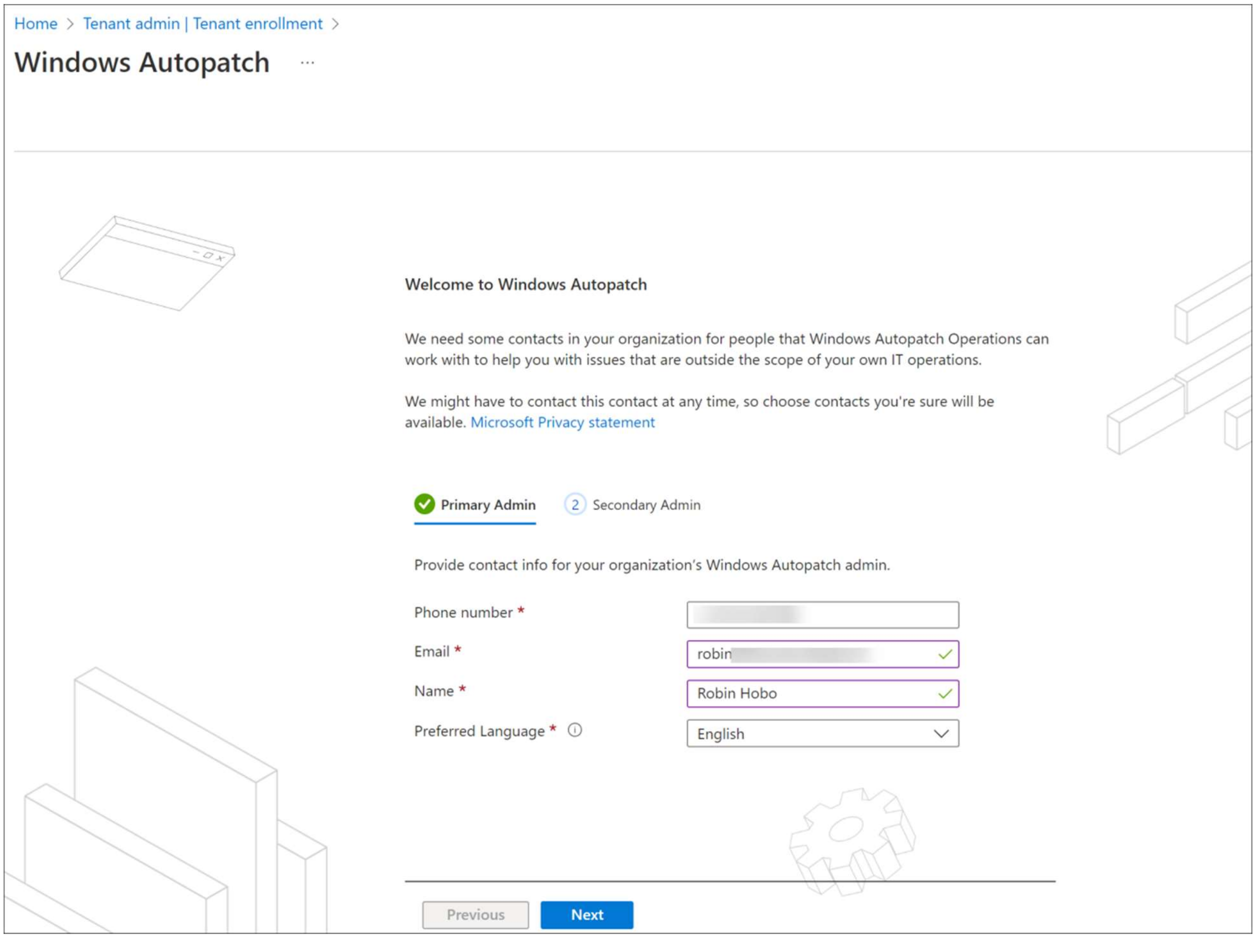
Allow administrator access for Microsoft

To get started, Microsoft needs your permission to take a few actions in your Azure Active Directory organization and on devices you want to enroll in Windows Autopatch. With your permission, Microsoft will do the following:

- Create a Microsoft application that we use to run the Windows Autopatch service. Learn more about Windows Autopatch enterprise applications
- Create the policies, groups and scripts necessary to run the service. This involves excluding necessary for any of your existing policies that may cause conflicts. Windows Autopatch update policies must take precedence to avoid any conflicts. Learn more about Changes made at tenant enrollment
- Manage devices using Intune.
- Collect and share info on usage, status, and compliance for devices and apps.
- Collect and share Windows Diagnostic data on usage, status, and compliance for devices and apps. Learn more about the data we collect
- Store Windows Autopatch data securely in Azure data centers based on your data residency. Learn more about Windows Autopatch data storage

☑ I give Microsoft permission to manage my Azure AD organization on my behalf.
Revoking this access at any point terminates the service.

Select **I give Microsoft permission to manage my Azure AD organization on my behalf** (if you do) and click **Agree**



Home > Tenant admin | Tenant enrollment >

Windows Autopatch ...

Welcome to Windows Autopatch

We need some contacts in your organization for people that Windows Autopatch Operations can work with to help you with issues that are outside the scope of your own IT operations.

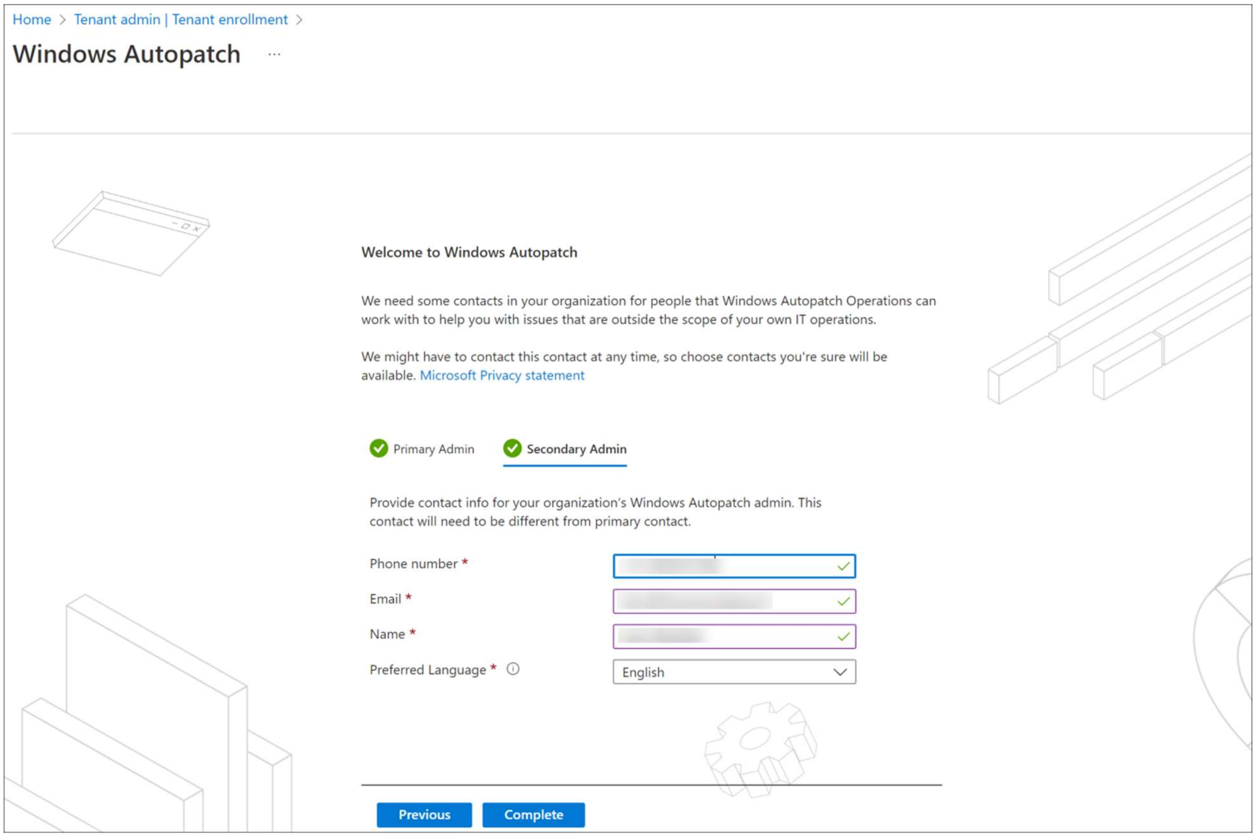
We might have to contact this contact at any time, so choose contacts you're sure will be available. Microsoft Privacy statement

✓ Primary Admin   2 Secondary Admin

Provide contact info for your organization's Windows Autopatch admin.

Phone number *	[redacted]
Email *	robin[redacted] ✓
Name *	Robin Hobo ✓
Preferred Language * ⓘ	English

Fill in the primary admin contact details and click **Next**



Home > Tenant admin | Tenant enrollment >

Windows Autopatch ...

Welcome to Windows Autopatch

We need some contacts in your organization for people that Windows Autopatch Operations can work with to help you with issues that are outside the scope of your own IT operations.

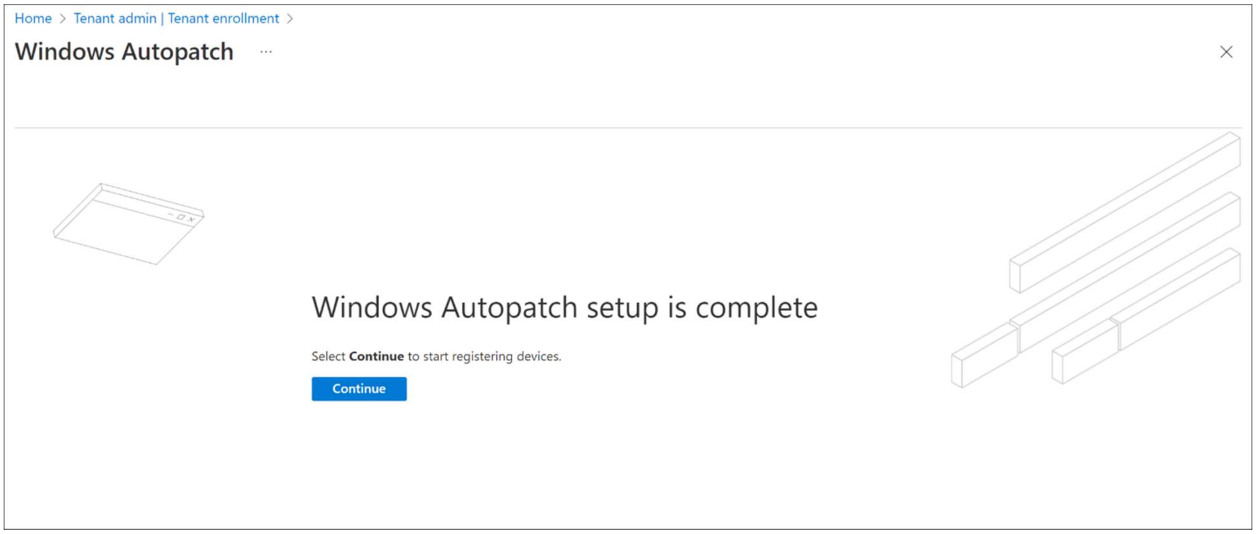
We might have to contact this contact at any time, so choose contacts you're sure will be available. Microsoft Privacy statement

✓ Primary Admin ✓ Secondary Admin

Provide contact info for your organization's Windows Autopatch admin. This contact will need to be different from primary contact.

Phone number *	[redacted] ✓
Email *	[redacted] ✓
Name *	[redacted] ✓
Preferred Language * ⓘ	English ⌄

Fill in the secondary admin contact details and click **Next**



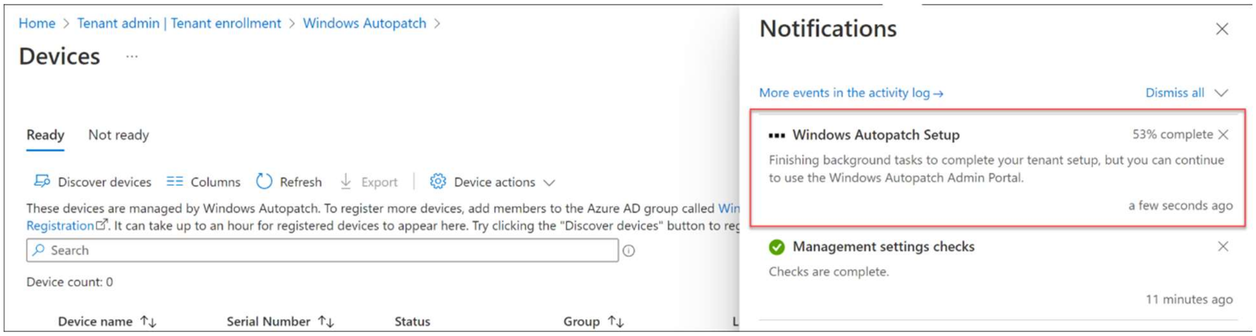
Home > Tenant admin | Tenant enrollment >

Windows Autopatch ...

Windows Autopatch setup is complete

Select **Continue** to start registering devices.

Click **Continue**



These devices are managed by Windows Autopatch. To register more devices, add members to the Azure AD group called Win
Registration. It can take up to an hour for registered devices to appear here. Try clicking the "Discover devices" button to reg

Device count: 0

Windows Autopatch Setup 53% complete

Finishing background tasks to complete your tenant setup, but you can continue to use the Windows Autopatch Admin Portal.

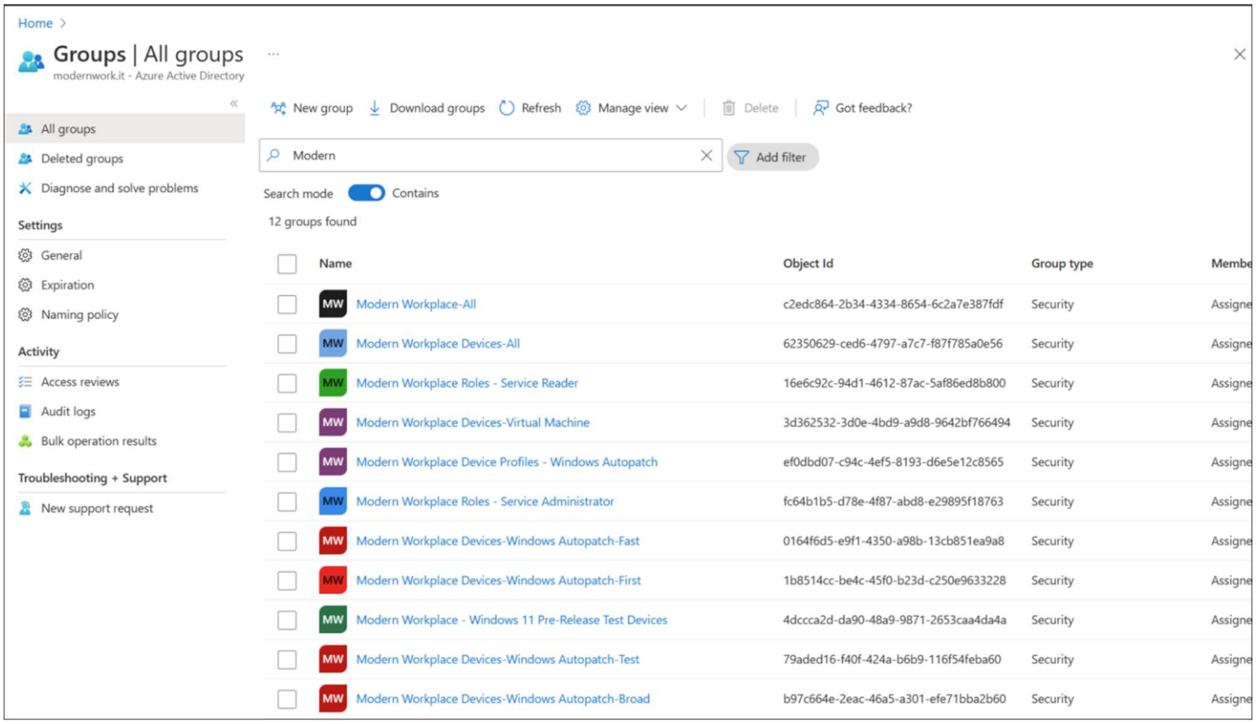
a few seconds ago

Management settings checks

Checks are complete.

11 minutes ago

In the background the resources will now be provisioned, this include security groups in Azure AD and policies in Microsoft Intune.



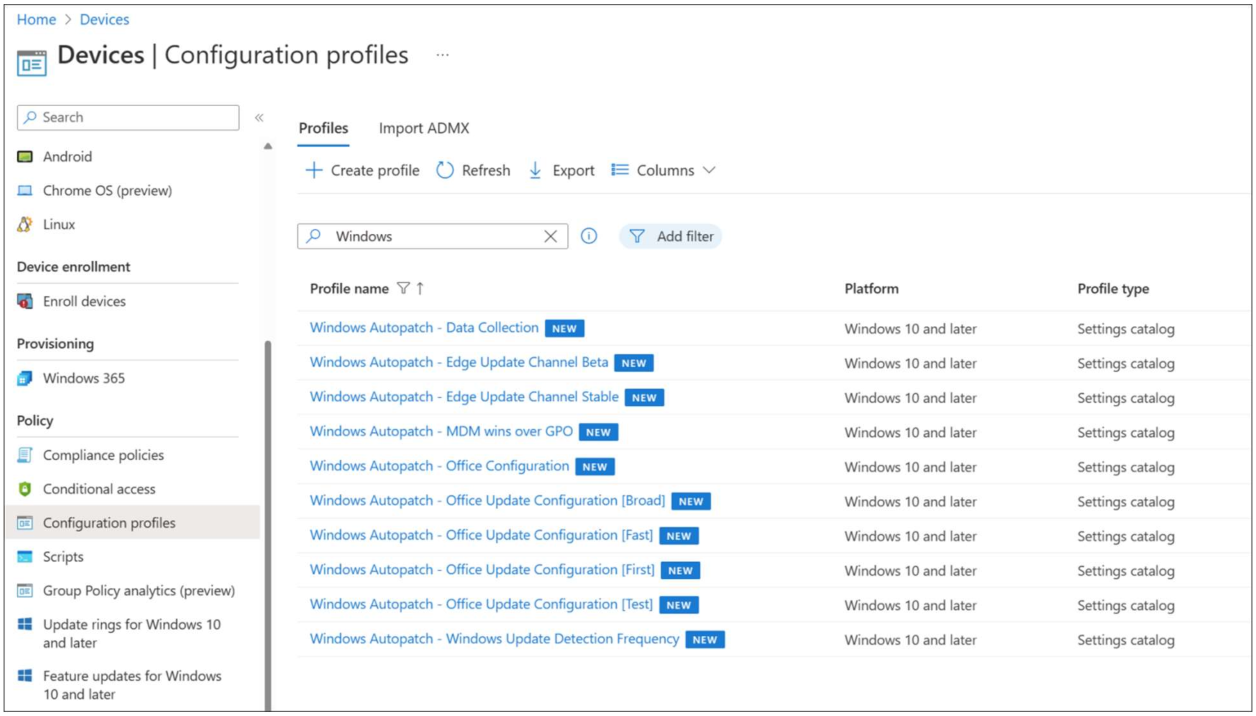
Search: Modern

Search mode: Contains

12 groups found

Name	Object Id	Group type	Membe
Modern Workplace-All	c2edc864-2b34-4334-8654-6c2a7e387fdf	Security	Assigne
Modern Workplace Devices-All	62350629-ced6-4797-a7c7-f87f785a0e56	Security	Assigne
Modern Workplace Roles - Service Reader	16e6c92c-94d1-4612-87ac-5af86ed8b800	Security	Assigne
Modern Workplace Devices-Virtual Machine	3d362532-3d0e-4bd9-a9d8-9642bf766494	Security	Assigne
Modern Workplace Device Profiles - Windows Autopatch	ef0dbd07-c94c-4ef5-8193-d6e5e12c8565	Security	Assigne
Modern Workplace Roles - Service Administrator	fc64b1b5-d78e-4f87-abd8-e29895f18763	Security	Assigne
Modern Workplace Devices-Windows Autopatch-Fast	0164f6d5-e9f1-4350-a98b-13cb851ea9a8	Security	Assigne
Modern Workplace Devices-Windows Autopatch-First	1b8514cc-be4c-45f0-b23d-c250e9633228	Security	Assigne
Modern Workplace - Windows 11 Pre-Release Test Devices	4dccca2d-da90-48a9-9871-2653caa4da4a	Security	Assigne
Modern Workplace Devices-Windows Autopatch-Test	79aded16-f40f-424a-b6b9-116f54feba60	Security	Assigne
Modern Workplace Devices-Windows Autopatch-Broad	b97c664e-2eac-46a5-a301-efe71bba2b60	Security	Assigne

In Azure AD the groups in the above screenshot are created during the Windows Autopatch deployment.

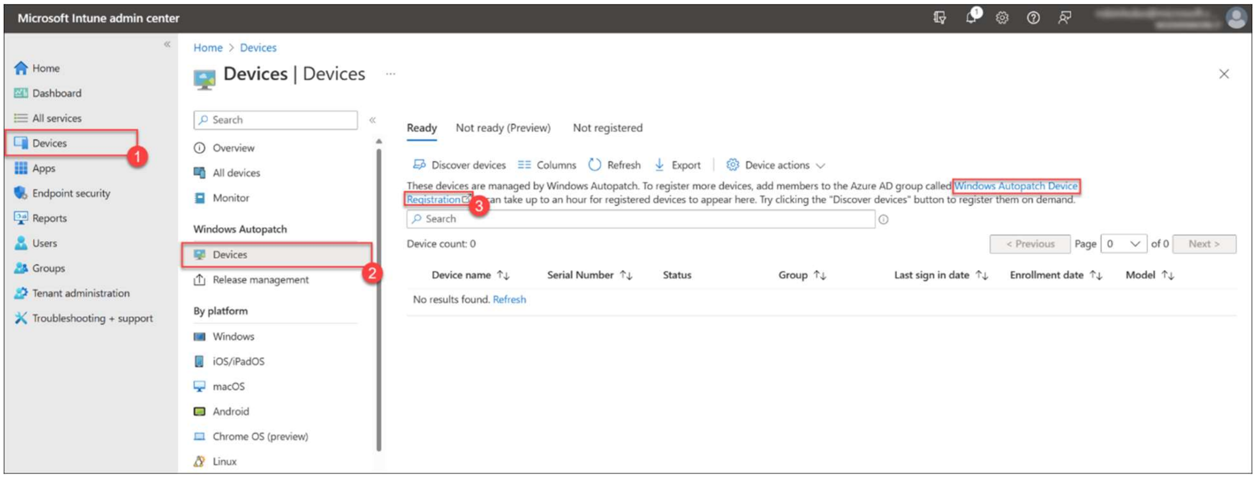


Profile name	Platform	Profile type
Windows Autopatch - Data Collection NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Edge Update Channel Beta NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Edge Update Channel Stable NEW	Windows 10 and later	Settings catalog
Windows Autopatch - MDM wins over GPO NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Office Configuration NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Office Update Configuration [Broad] NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Office Update Configuration [Fast] NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Office Update Configuration [First] NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Office Update Configuration [Test] NEW	Windows 10 and later	Settings catalog
Windows Autopatch - Windows Update Detection Frequency NEW	Windows 10 and later	Settings catalog

The Configuration profiles for Windows endpoints are created during the Windows Autopatch deployment. Beside these policies, also **Update rings for Windows 10 and later** and **Feature updates for Windows 10 and later** polices are created.

2 – Onboard devices to Windows Autopatch

To register / onboard devices to Windows Autopatch you need to make the devices member of the **Windows Autopatch Device Registration** security group.

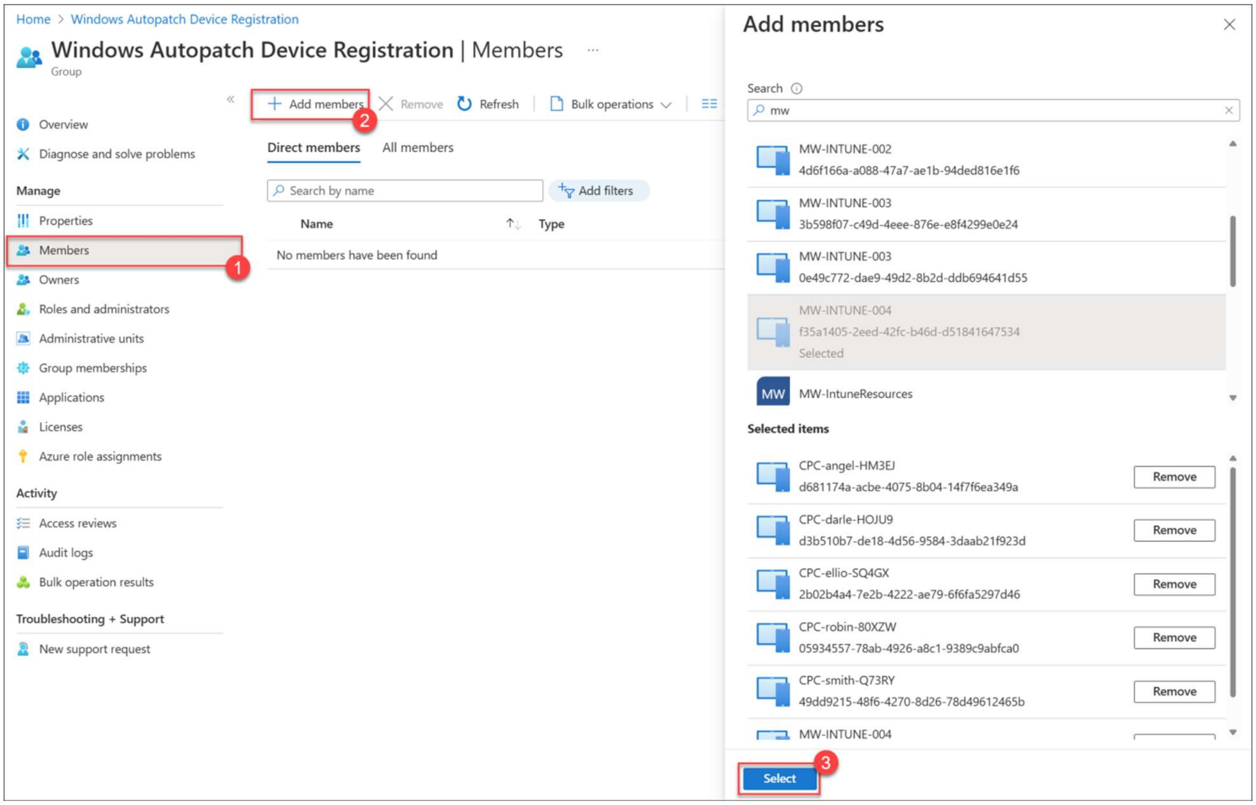


These devices are managed by Windows Autopatch. To register more devices, add members to the Azure AD group called Windows Autopatch Device Registration. It can take up to an hour for registered devices to appear here. Try clicking the "Discover devices" button to register them on demand.

Device count: 0

Device name	Serial Number	Status	Group	Last sign in date	Enrollment date	Model
No results found. Refresh						

Within the Microsoft Intune admin center, navigate to **Devices > Windows Autopatch Devices**. Click **Windows Autopatch Device Registration.**



No members have been found

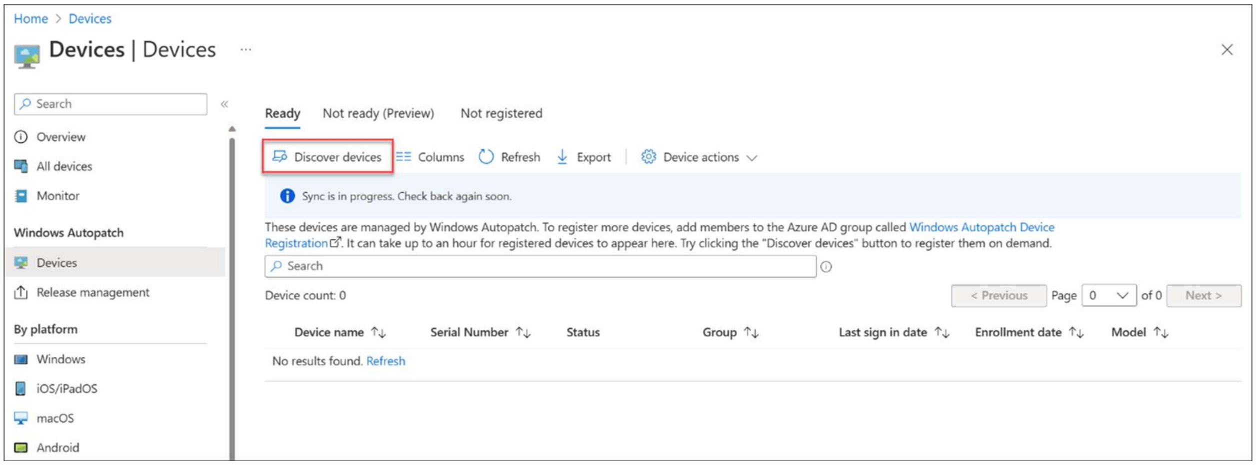
Search: mw

MW-INTUNE-002	4d6f166a-a088-47a7-ae1b-94ded816e1f6
MW-INTUNE-003	3b598f07-c49d-4eee-876e-e8f4299e0e24
MW-INTUNE-003	0e49c772-dae9-49d2-8b2d-ddb694641d55
MW-INTUNE-004	f35a1405-2eed-42fc-b46d-d51841647534 Selected
MW-IntuneResources	

Selected items

CPC-angel-HM3EJ	d681174a-acbe-4075-8b04-14f7f6ea349a
CPC-darle-HOJU9	d3b510b7-de18-4d56-9584-3daab21f923d
CPC-ellio-SQ4GX	2b02b4a4-7e2b-4222-ae79-6f6fa5297d46
CPC-robin-80XZW	05934557-78ab-4926-a8c1-9389c9abfca0
CPC-smith-Q73RY	49dd9215-48f6-4270-8d26-78d49612465b
MW-INTUNE-004	

With that link the **Windows Autopatch Device Registration** security group will be opened in a new browser tab. Make sure the **Members** page is open and click **Add members** to add the computer accounts.



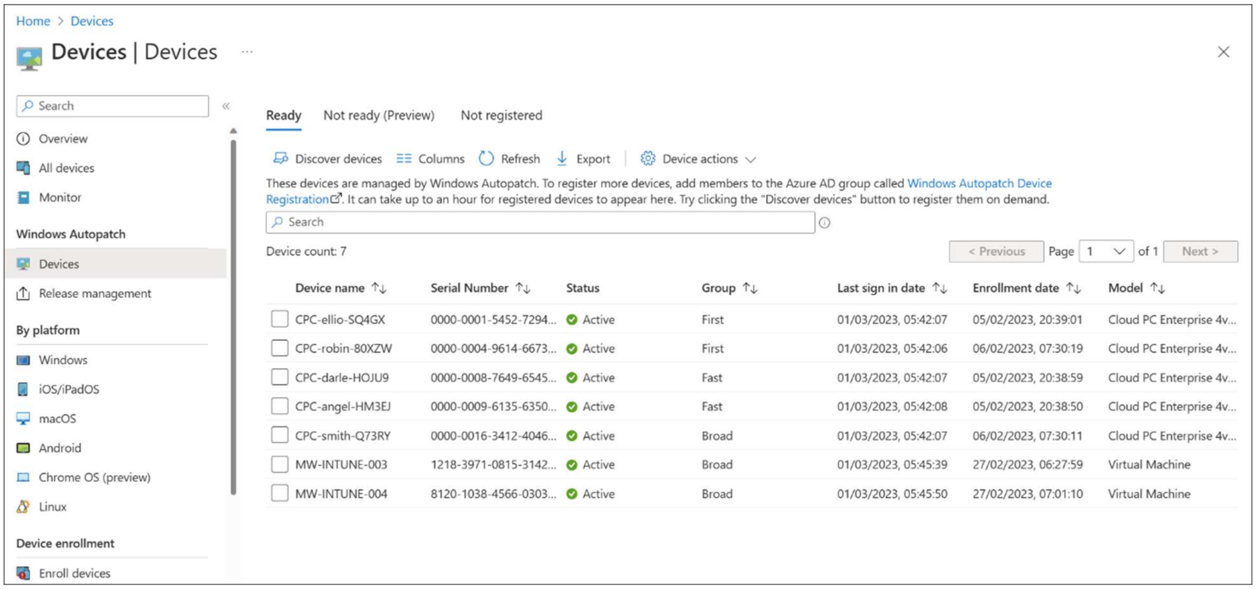
Sync is in progress. Check back again soon.

These devices are managed by Windows Autopatch. To register more devices, add members to the Azure AD group called Windows Autopatch Device Registration. It can take up to an hour for registered devices to appear here. Try clicking the "Discover devices" button to register them on demand.

Device count: 0

Device name	Serial Number	Status	Group	Last sign in date	Enrollment date	Model
No results found. Refresh						

Go back to the **Microsoft Intune admin center** and click on **Discover devices**



These devices are managed by Windows Autopatch. To register more devices, add members to the Azure AD group called Windows Autopatch Device Registration. It can take up to an hour for registered devices to appear here. Try clicking the "Discover devices" button to register them on demand.

Device count: 7

	Device name	Serial Number	Status	Group	Last sign in date	Enrollment date	Model
□	CPC-ellio-SQ4GX	0000-0001-5452-7294...	✓ Active	First	01/03/2023, 05:42:07	05/02/2023, 20:39:01	Cloud PC Enterprise 4v...
□	CPC-robin-80XZW	0000-0004-9614-6673...	✓ Active	First	01/03/2023, 05:42:06	06/02/2023, 07:30:19	Cloud PC Enterprise 4v...
□	CPC-darle-HOJU9	0000-0008-7649-6545...	✓ Active	Fast	01/03/2023, 05:42:07	05/02/2023, 20:38:59	Cloud PC Enterprise 4v...
□	CPC-angel-HM3EJ	0000-0009-6135-6350...	✓ Active	Fast	01/03/2023, 05:42:08	05/02/2023, 20:38:50	Cloud PC Enterprise 4v...
□	CPC-smith-Q73RY	0000-0016-3412-4046...	✓ Active	Broad	01/03/2023, 05:42:07	06/02/2023, 07:30:11	Cloud PC Enterprise 4v...
□	MW-INTUNE-003	1218-3971-0815-3142...	✓ Active	Broad	01/03/2023, 05:45:39	27/02/2023, 06:27:59	Virtual Machine
□	MW-INTUNE-004	8120-1038-4566-0303...	✓ Active	Broad	01/03/2023, 05:45:50	27/02/2023, 07:01:10	Virtual Machine

Once the device is onboarded to the Windows Autopatch service you can see which ring is assigned to the device.

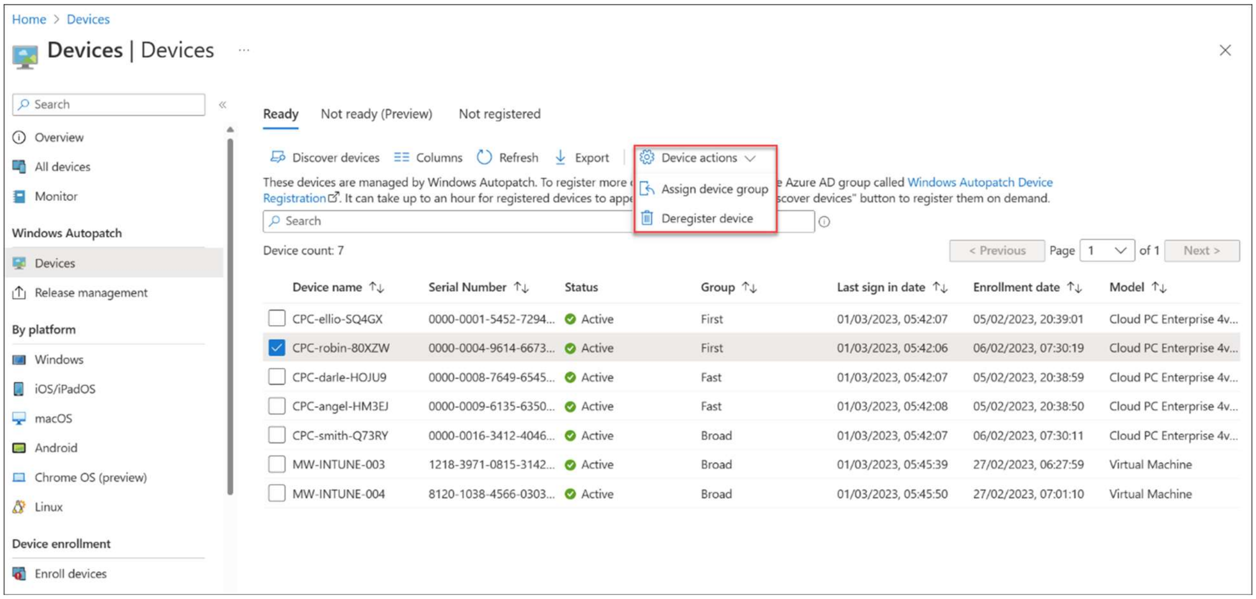
This can be one of the following rings.

Test – **Deployment** ring for testing update prior production rollout.

First -Early adopters

Fast – Quick rollout and adoption

Broad – Final ring for broad rollout

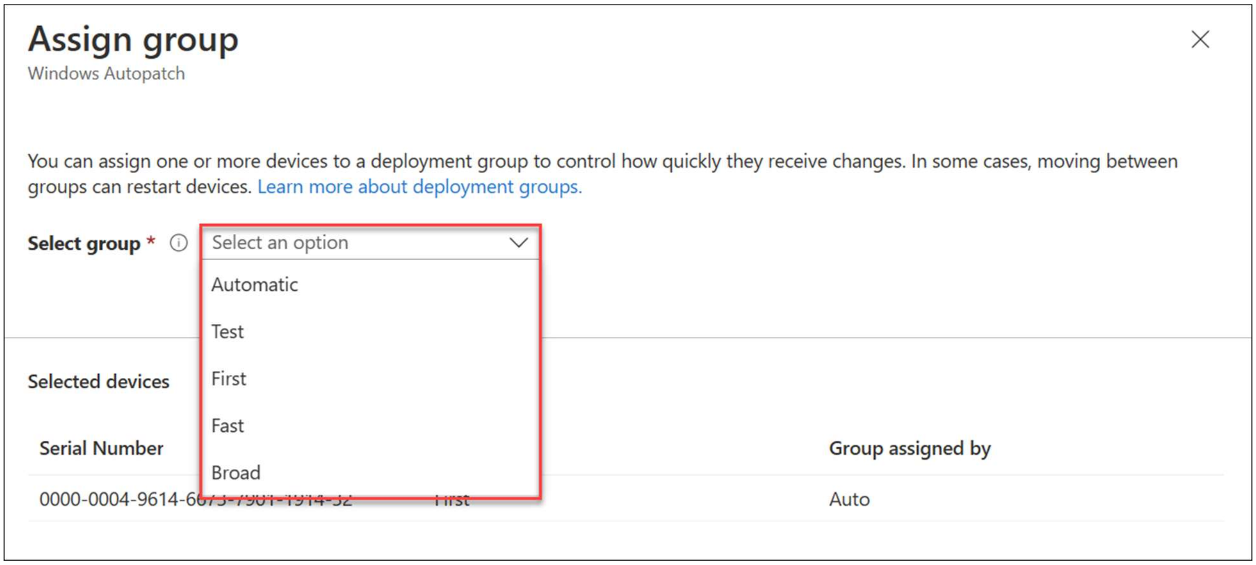


These devices are managed by Windows Autopatch. To register more ... e Azure AD group called Windows Autopatch Device Registration. It can take up to an hour for registered devices to appe... scover devices" button to register them on demand.

Device count: 7

	Device name	Serial Number	Status	Group	Last sign in date	Enrollment date	Model
☐	CPC-ellio-SQ4GX	0000-0001-5452-7294...	✓ Active	First	01/03/2023, 05:42:07	05/02/2023, 20:39:01	Cloud PC Enterprise 4v...
☑	CPC-robin-80XZW	0000-0004-9614-6673...	✓ Active	First	01/03/2023, 05:42:06	06/02/2023, 07:30:19	Cloud PC Enterprise 4v...
☐	CPC-darle-HOJU9	0000-0008-7649-6545...	✓ Active	Fast	01/03/2023, 05:42:07	05/02/2023, 20:38:59	Cloud PC Enterprise 4v...
☐	CPC-angel-HM3EJ	0000-0009-6135-6350...	✓ Active	Fast	01/03/2023, 05:42:08	05/02/2023, 20:38:50	Cloud PC Enterprise 4v...
☐	CPC-smith-Q73RY	0000-0016-3412-4046...	✓ Active	Broad	01/03/2023, 05:42:07	06/02/2023, 07:30:11	Cloud PC Enterprise 4v...
☐	MW-INTUNE-003	1218-3971-0815-3142...	✓ Active	Broad	01/03/2023, 05:45:39	27/02/2023, 06:27:59	Virtual Machine
☐	MW-INTUNE-004	8120-1038-4566-0303...	✓ Active	Broad	01/03/2023, 05:45:50	27/02/2023, 07:01:10	Virtual Machine

When a device is selected, you can go to **Device actions > Assign device group** to change the update ring.



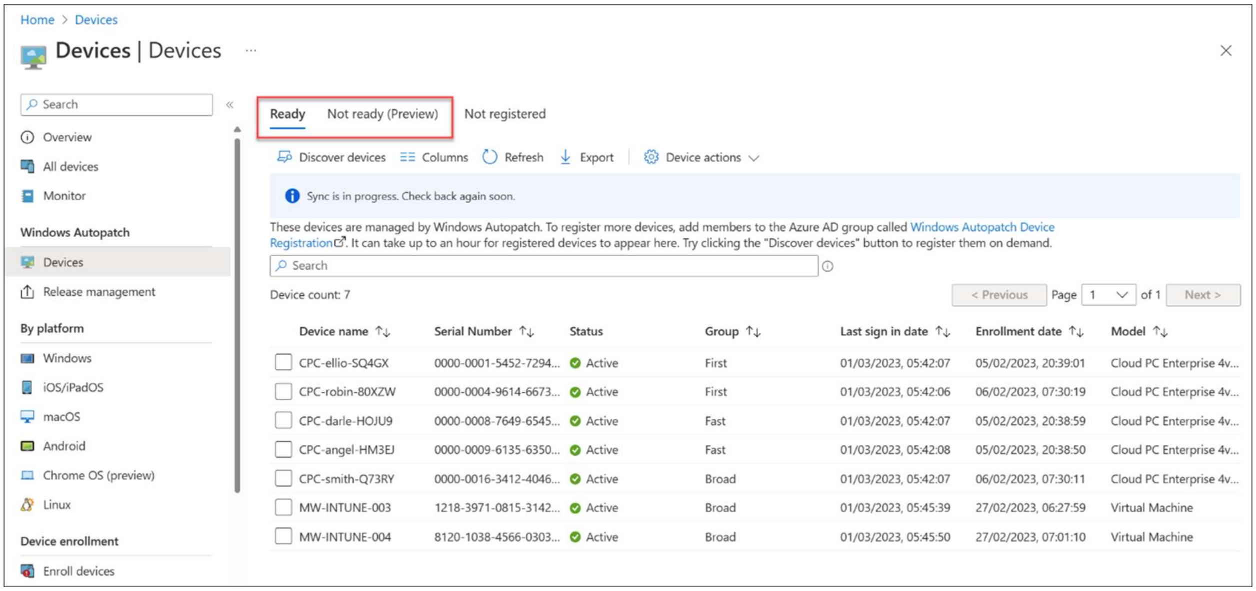
You can assign one or more devices to a deployment group to control how quickly they receive changes. In some cases, moving between groups can restart devices. Learn more about deployment groups.

Selected devices

Serial Number		Group assigned by
0000-0004-9614-6673-7901-1914-32	First	Auto

3 – Managing Windows Autopatch

I will give a short overview where you can manage Windows Autopatch within the Microsoft Intune admin center.



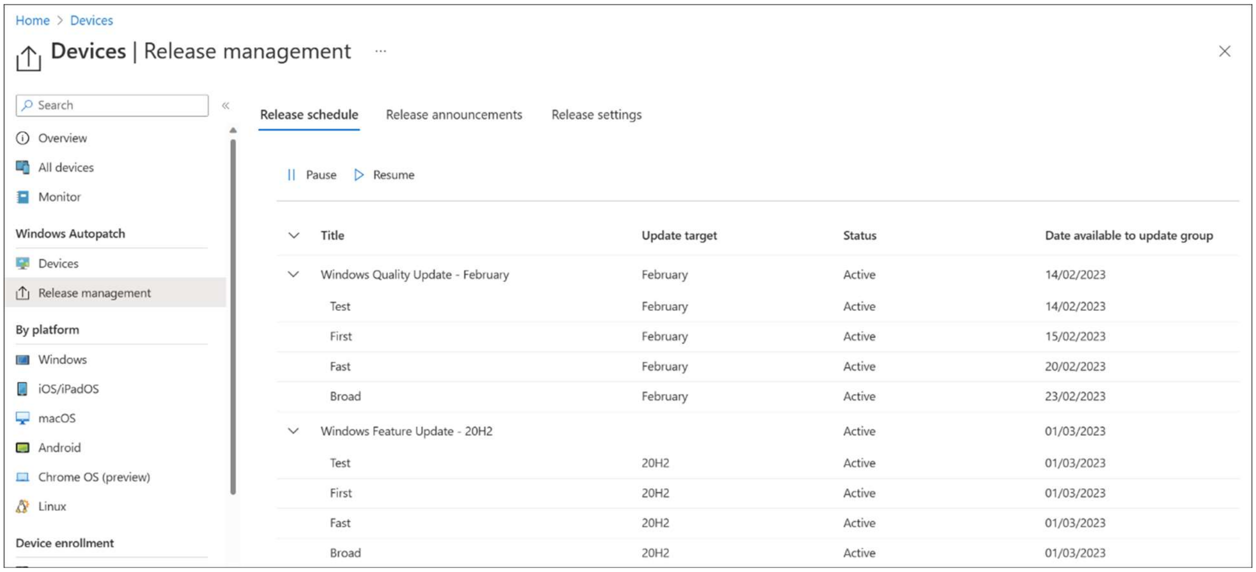
Sync is in progress. Check back again soon.

These devices are managed by Windows Autopatch. To register more devices, add members to the Azure AD group called Windows Autopatch Device Registration. It can take up to an hour for registered devices to appear here. Try clicking the "Discover devices" button to register them on demand.

Device count: 7

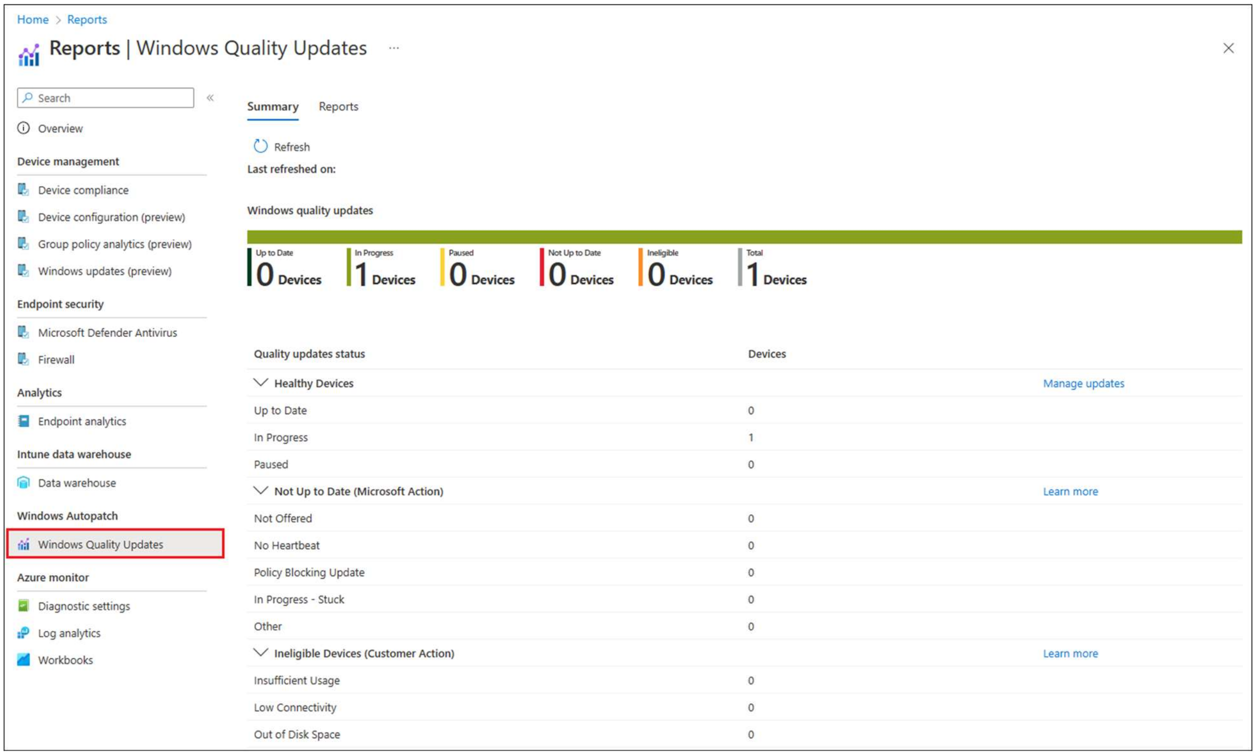
	Device name ↑↓	Serial Number ↑↓	Status	Group ↑↓	Last sign in date ↑↓	Enrollment date ↑↓	Model ↑↓
□	CPC-ellio-SQ4GX	0000-0001-5452-7294...	✓ Active	First	01/03/2023, 05:42:07	05/02/2023, 20:39:01	Cloud PC Enterprise 4v...
□	CPC-robin-80XZW	0000-0004-9614-6673...	✓ Active	First	01/03/2023, 05:42:06	06/02/2023, 07:30:19	Cloud PC Enterprise 4v...
□	CPC-darle-HOJU9	0000-0008-7649-6545...	✓ Active	Fast	01/03/2023, 05:42:07	05/02/2023, 20:38:59	Cloud PC Enterprise 4v...
□	CPC-angel-HM3EJ	0000-0009-6135-6350...	✓ Active	Fast	01/03/2023, 05:42:08	05/02/2023, 20:38:50	Cloud PC Enterprise 4v...
□	CPC-smith-Q73RY	0000-0016-3412-4046...	✓ Active	Broad	01/03/2023, 05:42:07	06/02/2023, 07:30:11	Cloud PC Enterprise 4v...
□	MW-INTUNE-003	1218-3971-0815-3142...	✓ Active	Broad	01/03/2023, 05:45:39	27/02/2023, 06:27:59	Virtual Machine
□	MW-INTUNE-004	8120-1038-4566-0303...	✓ Active	Broad	01/03/2023, 05:45:50	27/02/2023, 07:01:10	Virtual Machine

Under devices a **Windows Autopatch** section has been added after the enrollment. In the **Devices** tab you can see an overview of devices that are **Ready** (onboarded) and **Not ready**. A reason that a device is Not ready can be that prerequisites are not met.



Title	Update target	Status	Date available to update group
Windows Quality Update - February	February	Active	14/02/2023
Test	February	Active	14/02/2023
First	February	Active	15/02/2023
Fast	February	Active	20/02/2023
Broad	February	Active	23/02/2023
Windows Feature Update - 20H2		Active	01/03/2023
Test	20H2	Active	01/03/2023
First	20H2	Active	01/03/2023
Fast	20H2	Active	01/03/2023
Broad	20H2	Active	01/03/2023

On the **Release management** tab you have the option to **Pause** and **Resume** updates per ring. You can also see which updates are announced under the **Release announcements** tab. In the **Release settings** tab you can configure if you want to apply the **Expedited quality updates** and/or **Microsoft 365 apps update**s (enabled by default).



Home > Reports

Reports | Windows Quality Updates ...

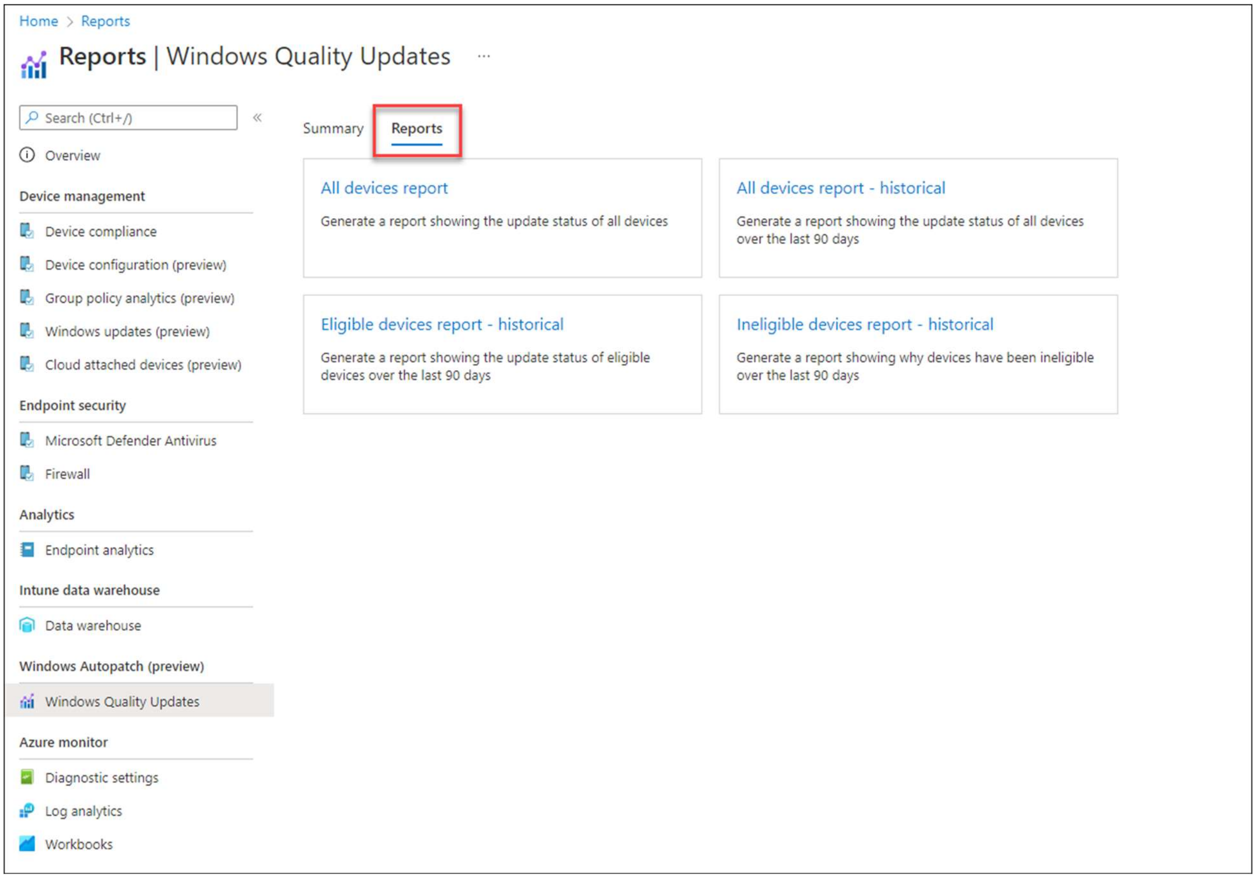
Last refreshed on:

Windows quality updates

Up to Date	In Progress	Paused	Not Up to Date	Ineligible	Total
0 Devices	1 Devices	0 Devices	0 Devices	0 Devices	1 Devices

Quality updates status	Devices	
Healthy Devices		Manage updates
Up to Date	0	
In Progress	1	
Paused	0	
Not Up to Date (Microsoft Action)		Learn more
Not Offered	0	
No Heartbeat	0	
Policy Blocking Update	0	
In Progress - Stuck	0	
Other	0	
Ineligible Devices (Customer Action)		Learn more
Insufficient Usage	0	
Low Connectivity	0	
Out of Disk Space	0	

In the Microsoft Intune admin center, under **Reports** you can also find a new section regarding Windows Autopatch; **Windows Quality Updates**. This gives an overview on all the device statuses (can take a few hours before this report is up to date).



Reports | Windows Quality Updates

All devices report

Generate a report showing the update status of all devices

All devices report - historical

Generate a report showing the update status of all devices over the last 90 days

Eligible devices report - historical

Generate a report showing the update status of eligible devices over the last 90 days

Ineligible devices report - historical

Generate a report showing why devices have been ineligible over the last 90 days

There are also **Reports** to display historical trends in your environment.

This was a short post about how to deploy Windows Autopatch followed by a short introduction about some management features.