HARDEN 365

Protect your data in minutes

Harden 365 – déploiement des mises à jour avec Intune (Windows Autopatch et les Rings)

Sommaire

1 Objectifs

Ce guide a pour but de présenter comment mettre à jour une machine jointe à Azure AD ou jointe de manière hybride avec Microsoft Intune. Deux solutions sont présentées dans ce document :

- Windows Autopatch
- Les Rings

2 Besoins, choix, configuration cible

2.1 Les besoins

Les clients ont besoin de mettre à jour :

- Microsoft 365 Apps for Enterprise
- Windows 10 E3 / Windows 10 E5
- Les navigateurs web comme Microsoft Edge ou Google Chrome

2.2 Les différents types de mise à jour Windows

2 types de mises à jour existent avec Windows 10 / 11 :

- Les mises à jour mensuelles cumulatives de qualité (*Quality update*) : il s'agit des mises à jour mensuelle pour le déploiement des correctifs de sécurités et des bugs. Les correctifs mensuels Windows Server sont cumulatifs depuis 2014. Les correctifs du mois en cours incluent ceux des mois précédents. https://www.howto-connect.com/difference-between-update-and-cumulative-windows-10/
- Les mises à jour de fonctionnalités (*Feature update*) : ce sont les changements de BUILD (passage de la 20H2 à la 21H2).

2.3 Choix des solutions techniques

La communauté préconise l'utilisation de *Windows Update*, *Windows Update For Business* (différer le déploiement des mises à jour de fonctionnalités et des mises à jour cumulatives mensuelles de qualité) et *Delivery Optimization* (système de cache pour optimiser la bande passante pour déployer les correctifs de sécurité).

Le paramétrage de ces solutions peut se faire à l'aide de GPO ou avec Microsoft Intune.

2 solutions sont disponibles pour gérer la mise à jour des machines Windows 10 / 11 avec Microsoft Intune :

- La solution *Windows Autopatch* : cette solution est préférable si vous disposez des abonnements *Windows Enterprise E3, Intune, Azure AD Premium P1*
- Les *Update Ring*, *Feature updates for Windows 10* et *Quality Updates for Windows 10 and Later* : cette solution est préconisée si vous ne disposez pas des licences permettant d'utiliser *Windows Autopatch*.

3 Solution 1 : *Windows Autopatch*

3.1 Présentation générale

Microsoft vient de sortir *Windows Autopatch*. Cette solution s'appuie sur les fonctionnalités *Update Rings*, *Features updates for Windows 10 and later*.

https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/

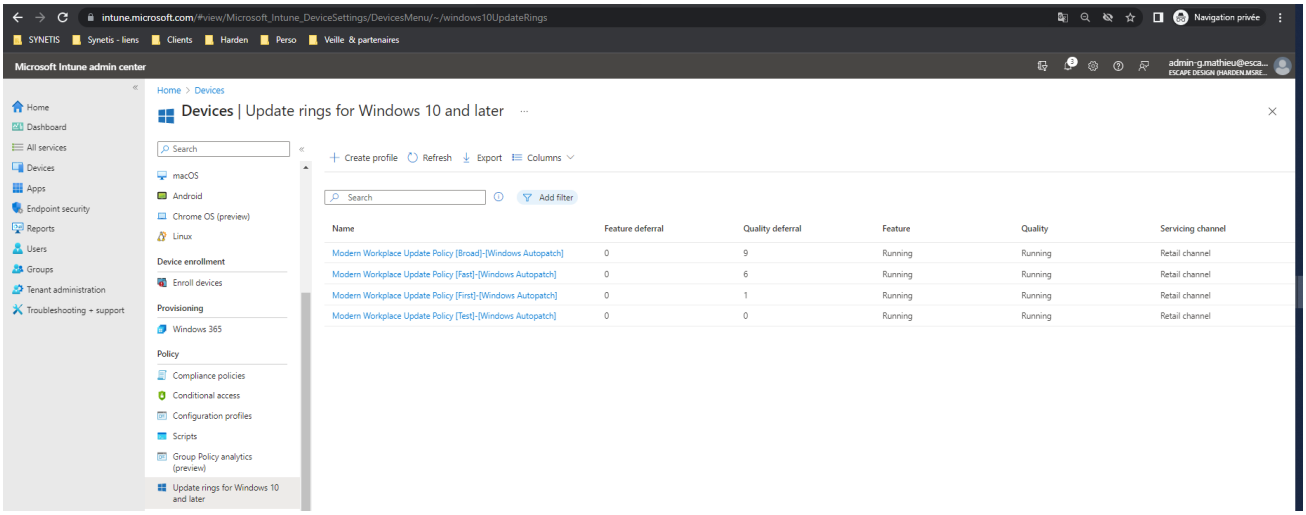
https://www.toutwindows.com/blogtoutwindows/intune-et-la-gestion-des-mises-a-jour-windows-wufb/

Elle permet uniquement de patcher des machines *Windows 10 1809* et versions supérieures, *Microsoft 365 Apps for Enterprise*, *Microsoft Edge* et *Microsoft Teams*. Elle nécessite des abonnements *Windows Enterprise E3*, *Intune*, *Azure AD Premium P1* (inclues dans l'abonnement *Microsoft 365 E3*).

Les ouvertures de flux sont requises vers les URL suivantes (TCP 443) :

- mmdcustomer.microsoft.com
- mmdls.microsoft.com
- logcollection.mmd.microsoft.com
- support.mmd.microsoft.com

La solution *Microsoft Autopatch* crée automatiquement 4 Updates Ring.

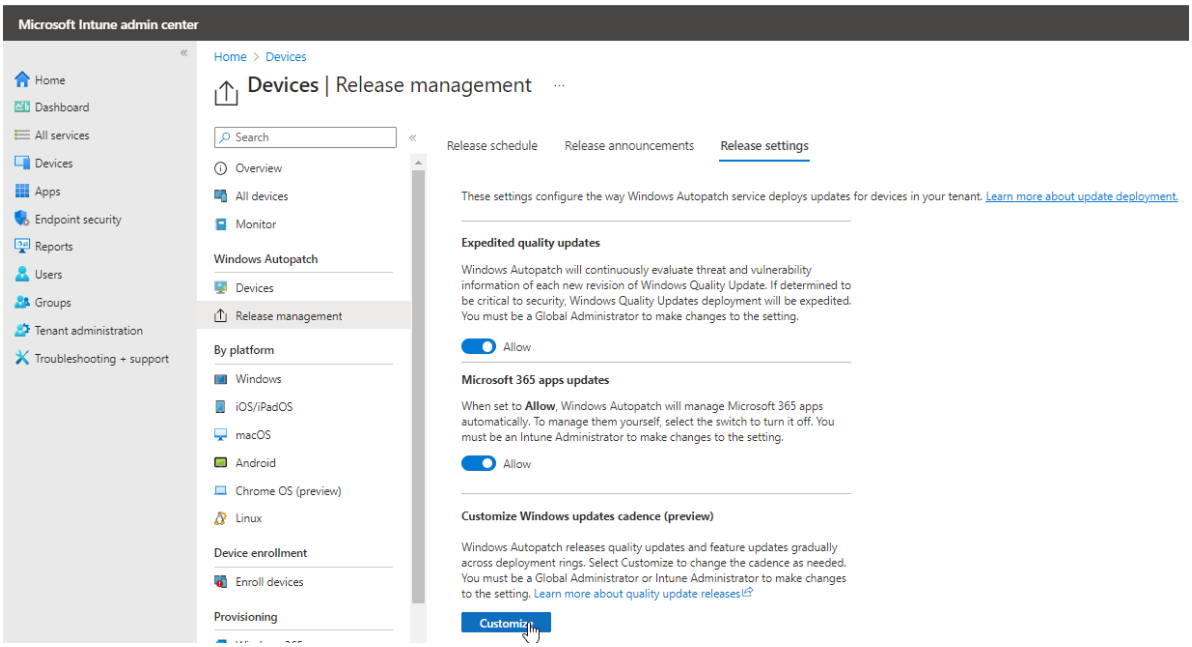


Par défaut, les mises à jour de fonctionnalités ne sont pas retardées et les correctifs mensuels sont retardés selon l'*Update Ring* (de 0 à 9 jours selon l'*Update Ring*).

Comme expliqué dans l'article https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/operate/windows-autopatch-windows-update, il est autorisé de modifier ces valeurs mais pas de modifier directement la configuration des *Update Ring* créés par *Windows Autopatch*.

You can customize the Windows Update deployment schedule for each deployment ring per your business and organizational needs. We recommend that you use the Windows Autopatch service default. However, you may have devices that need different schedules for updates deployment.

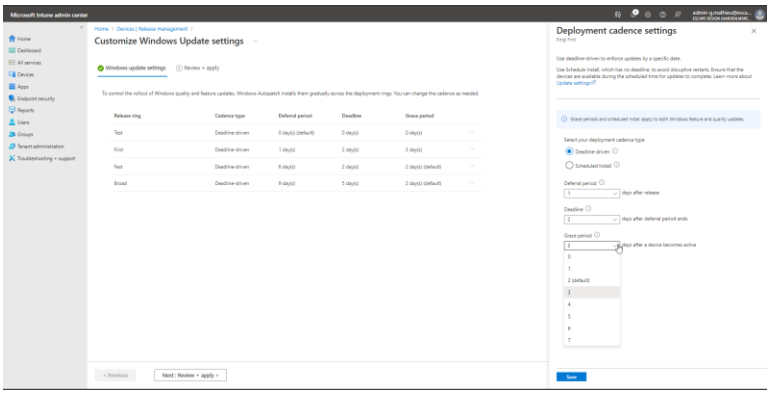
Il faut pour cela cliquer sur le bouton *Customize*.

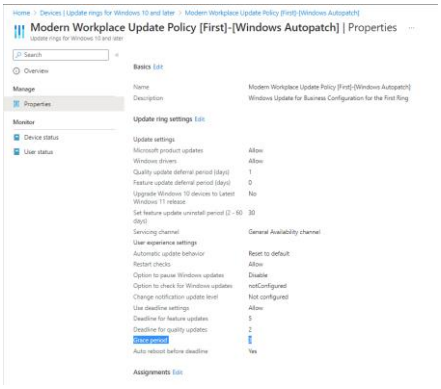


Le changement des règles de mises à jour se fait via le paramètre de *Deployment cadence settings*.

Un changement dans la configuration de ce paramètre met à jour l'*Update Ring* automatiquement.

La *Grace period* est passé de 2 à 3 jours dans cet exemple. Le changement est fait dans la capture de gauche et impacte la configuration du Ring (capture de droite).





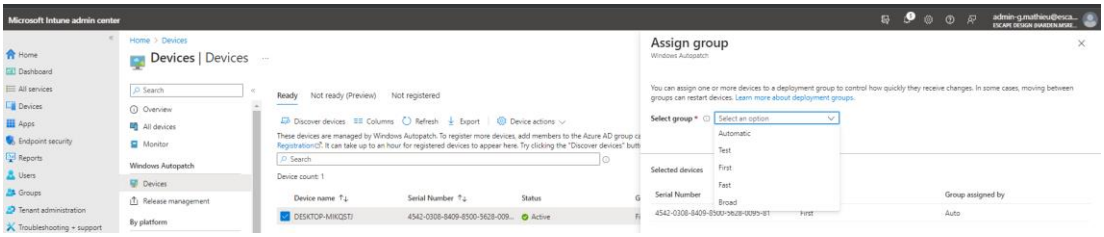
Avec *Windows Autopatch*, c'est Microsoft qui affecte les machines automatiquement dans les différents *Update Rings*. Le fait d'assigner les machines dans les Updates Rings créés par *Windows Autopatch* n'est pas supporté.

https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/operate/windows-autopatch-update-management

> ⚠ **Warning**
>
> Adding or importing devices into any of these groups directly is not supported and doing so might cause an unexpected impact on the Windows Autopatch service. To move devices between these groups, see **Moving devices in between deployment rings**.

Il faut utiliser une commande spéciale pour changer une machine de Ring.

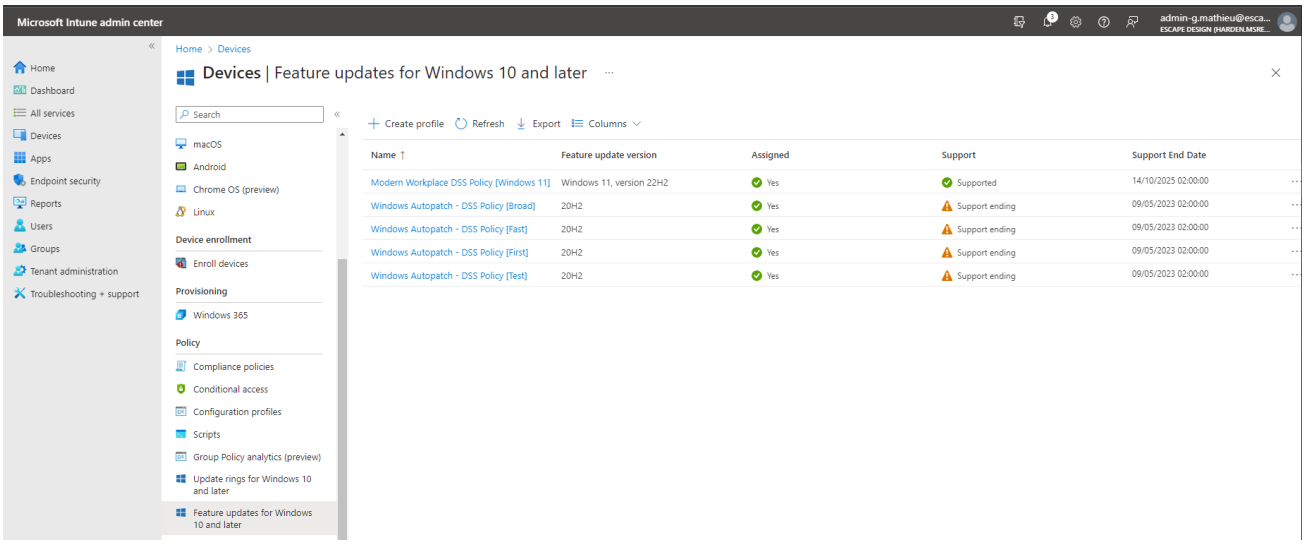
https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/operate/windows-autopatch-update-management#moving-devices-in-between-deployment-rings



> **Note**
>
> You can only move devices to other deployment rings when they're in an active state in the **Ready** tab.
>
> If you don't see the **Ring assigned by column** change to **Pending** in Step 5, check to see whether the device exists in Microsoft Intune or not by searching for it in its device blade. For more information, see **Device details in Intune**.

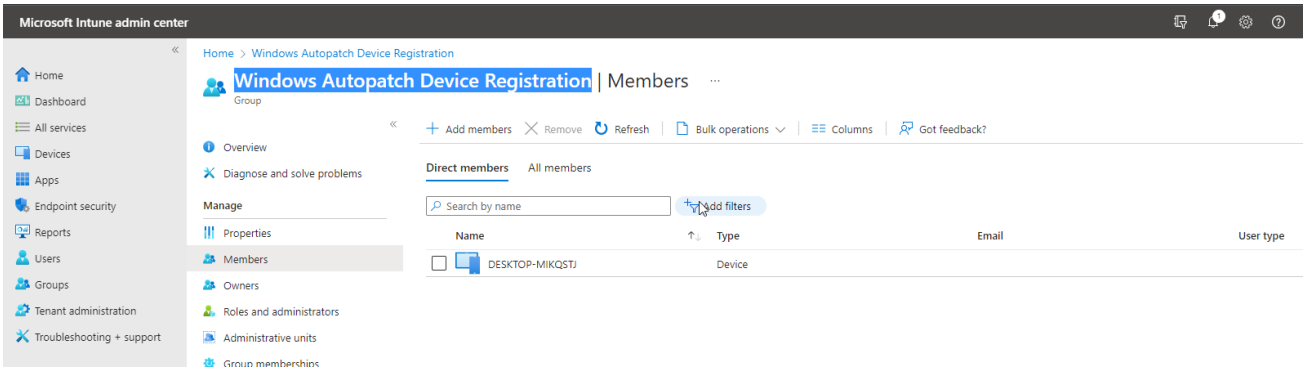
> **Warning**
>
> Moving devices between deployment rings through directly changing Azure AD group membership isn't supported and may cause unintended configuration conflicts within the Windows Autopatch service. To avoid service interruption to devices, use the **Assign device to ring** action described previously to move devices between deployment rings.

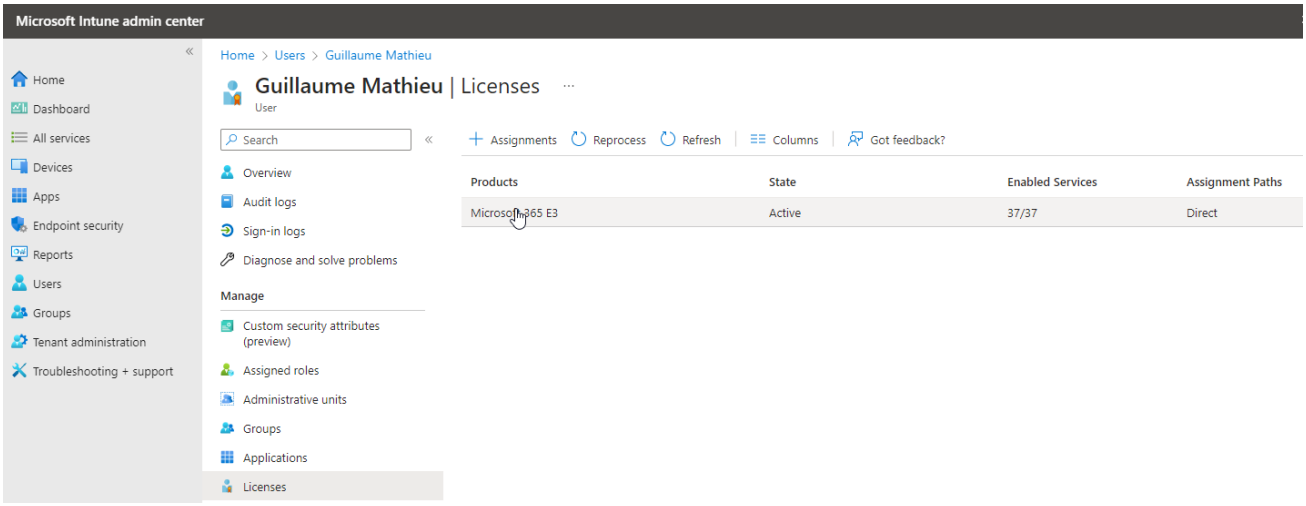
La solution *Windows Autopatch* crée aussi des règles pour forcer la mise à jour de machine avec une version non supportée de Windows vers une version spécifique de Windows 10 (20H2 dans l'exemple).



Il faut ensuite ajouter les machines dans le groupe *Windows Autopatch Device Registration*.

Les comptes utilisateurs Azure AD doivent aussi disposer d'une licence *Intune*, *Azure AD Premium* et *Windows Enterprise E3*.



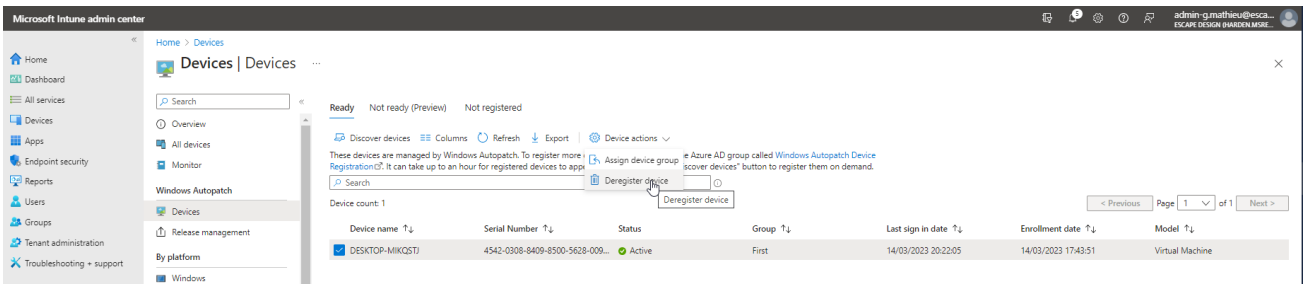


A savoir :

The Windows Autopatch Device Registration Azure AD group only supports one level of Azure AD nested groups.

Pour supprimer le fait que la solution *Windows Autopatch* arrêt de gérer une machine, il ne suffit pas de supprimer la machine du groupe *Windows Autopatch Device Registration*. Il faut utiliser la commande *Deregister device*.

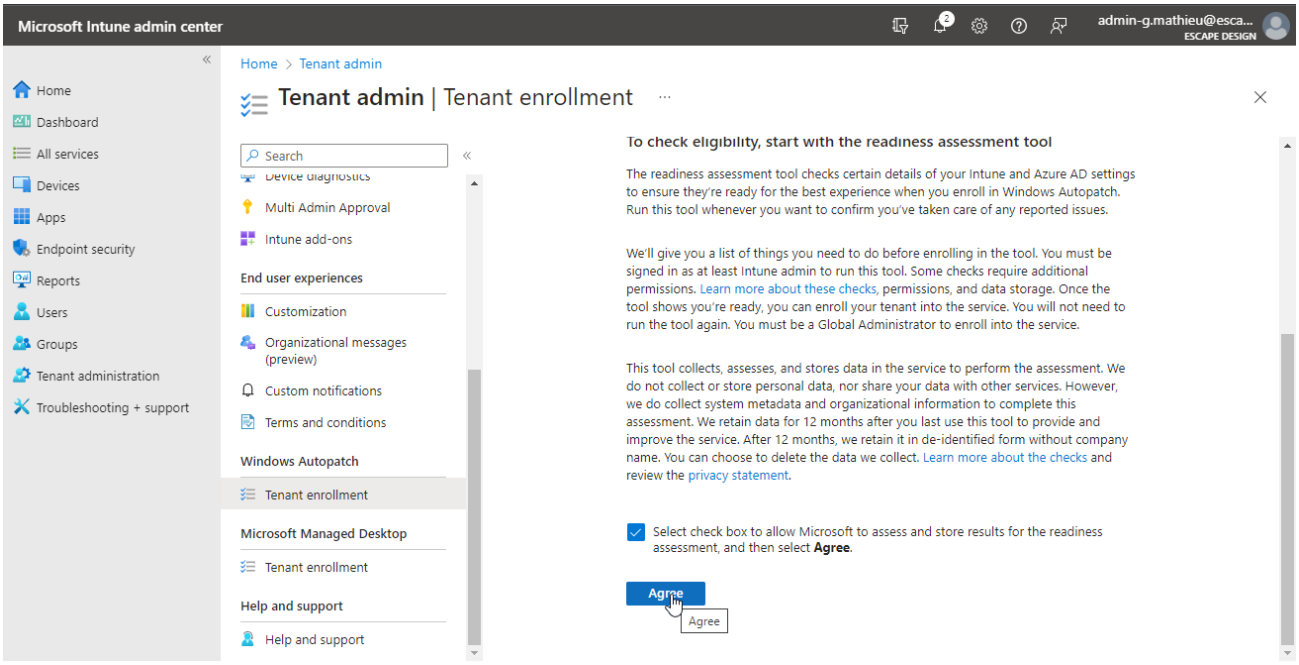
https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/operate/windows-autopatch-deregister-devices



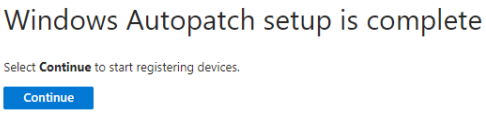
3.2 Déploiement de Windows Autopatch

La solution *Windows Autopatch* doit être activée sur le Tenant Microsoft 365.

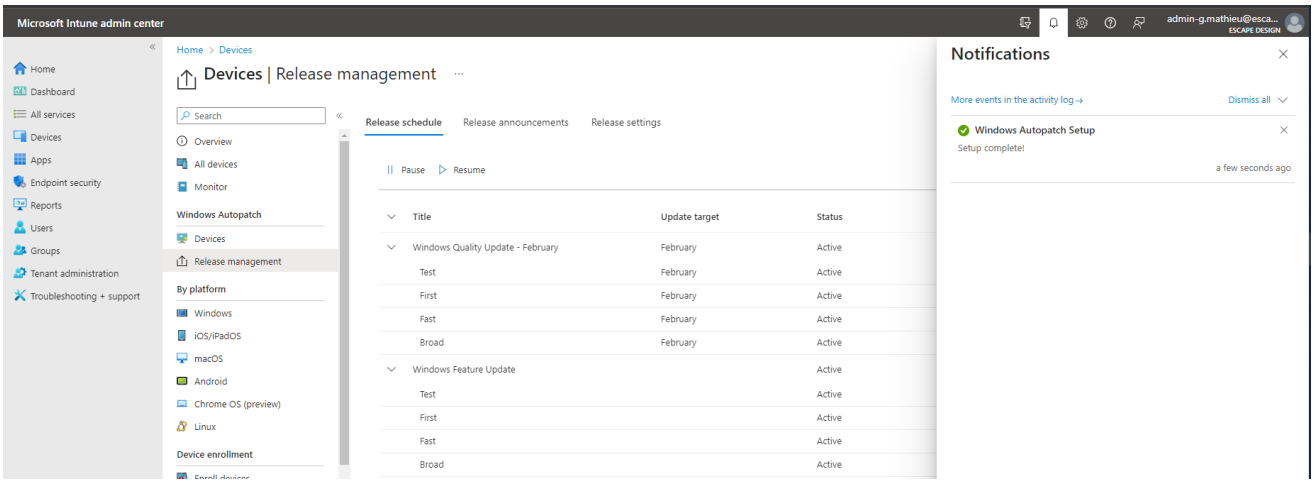
https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/prepare/windows-autopatch-enroll-tenant



Il faut renseigner le contacts d'au moins 2 personnes de l'équipe IT.



Un nouveau menu *Windows Autopach* apparaît alors.



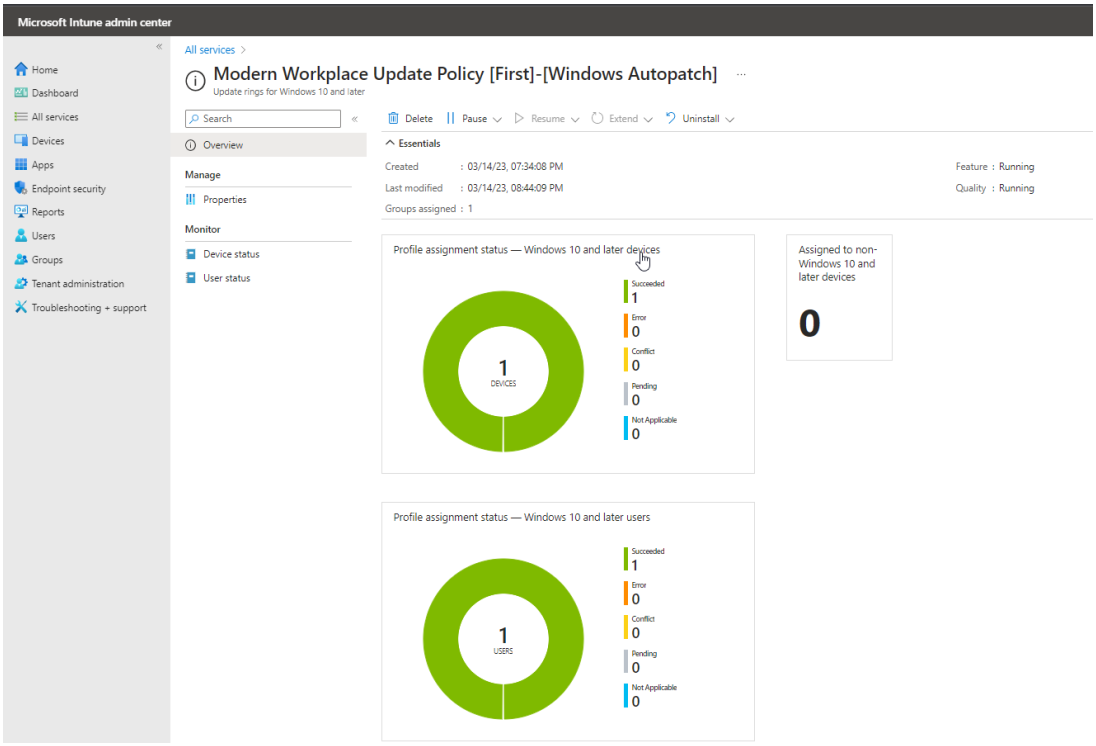
4 Solution 2 : Update Rings

4.1 Présentation générale

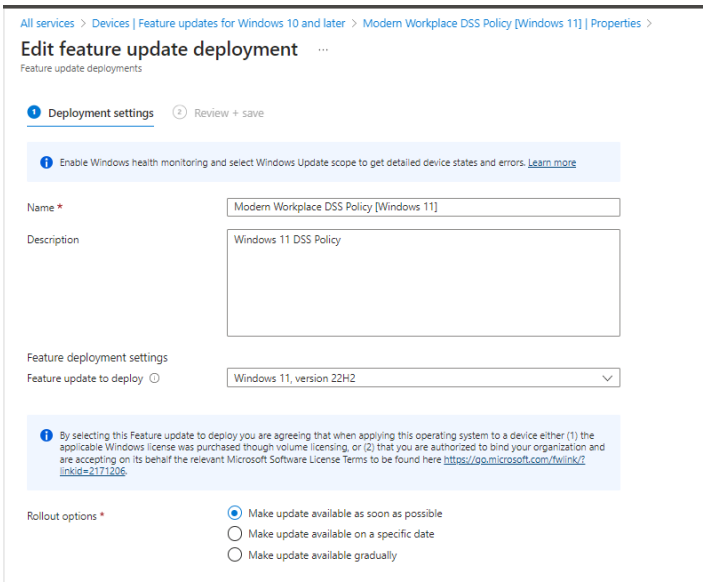
Il est possible de créer plusieurs Rings sur le modèle de la solution *Windows Autopatch*.

La configuration des mises à jour se fait en créant des *Update rings for Windows 10 and later*.

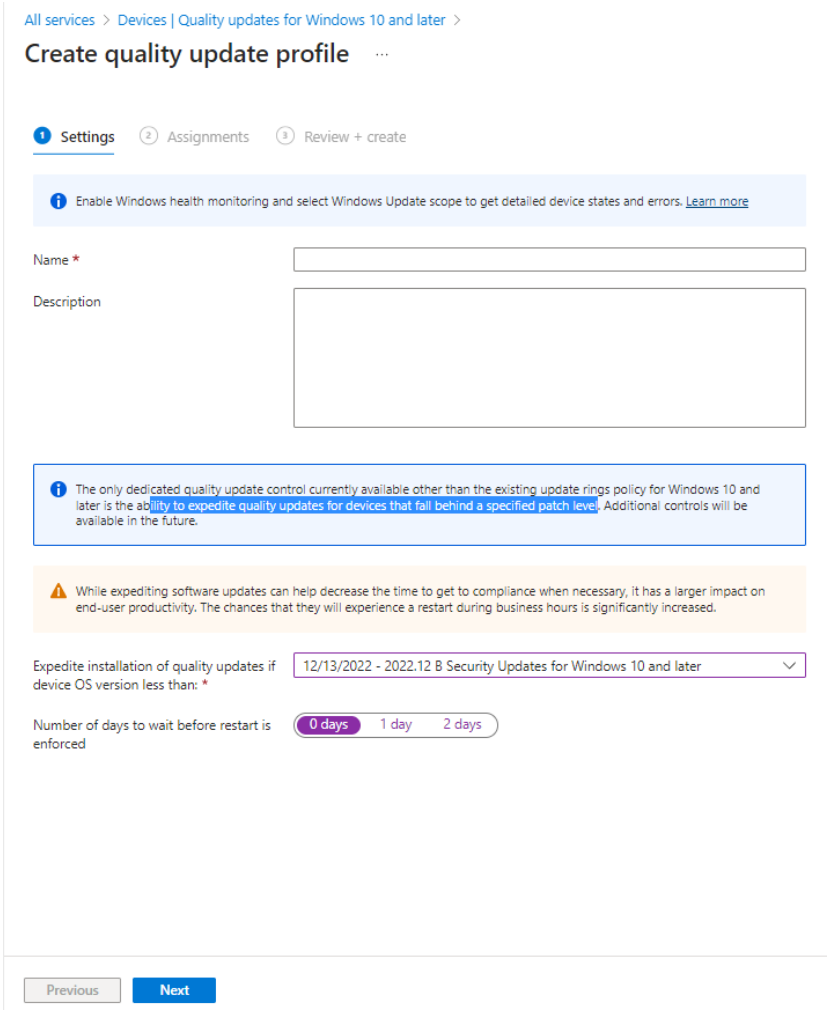
La vue d'ensemble permet de valider les machines à jour d'un Ring permet de voir les machines à jour ou non.



Le menu *Feature Update for Windows 10 and later* permet uniquement de forcer le fait de forcer des machines à se mettre à jour. Dans cet exemple, nous forçons les machines Windows 10 à se mettre à jour dès que possible vers Windows 11. La règle ci-dessous a été créée automatiquement par *Windows Autopatch*.



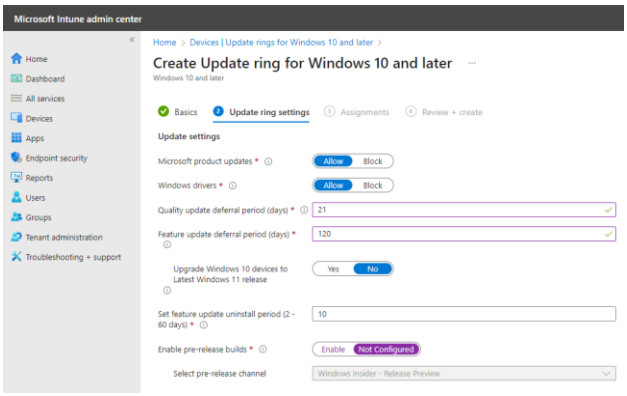
Sur le même principe, un *profil Quality Update* permet de forcer le déploiement d'un correctif cumulatif spécifique sur une machine qui rencontrerait des problèmes de déploiement.

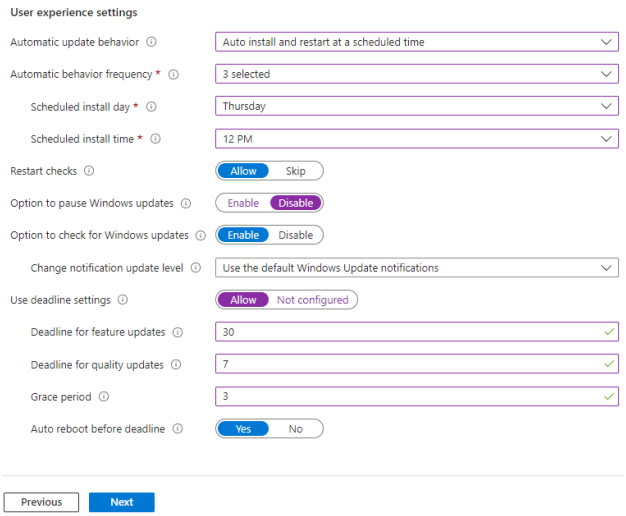


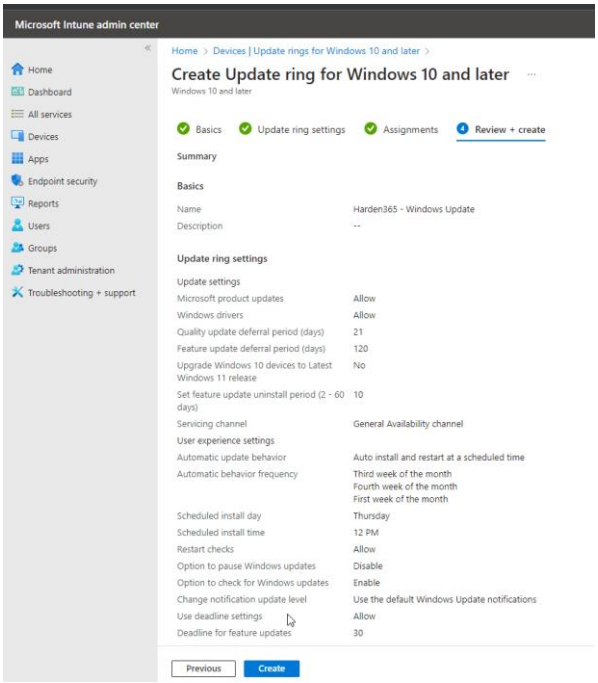
4.2 Création d'un Update Ring

Créer le profil *Harden365 - Windows Update*.

Les valeurs ci-dessous sont des valeurs exemples qui ne doivent pas être utilisés en production.







La configuration préconisée ci-dessous permet de retarder le déploiement des correctifs mensuels de 7 jours. Ce réglage permet d'éviter les problèmes avec certains correctifs mensuels.

Un principe similaire est appliqué pour les correctifs de type *feature update*.

L'installation se fera le jeudi midi toutes les semaines sauf la semaine 2 (celle où les correctifs sortent).

Il est préconisé de créer 4 Rings avec les mêmes paramètres de *Windows Autopatch*.

Vous pouvez activer une version d'évaluation de Microsoft 365 E3 pour disposer temporairement des licences requises pour activer *Windows Autopatch* sur un tenant de test et copier cette configuration manuellement sur votre Tenant de production.

Pour éviter tout conflit avec *Windows Autopatch*, toujours exclure le groupe Azure AD *Windows Autopatch Device Registration*.

https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/operate/windows-autopatch-maintain-environment