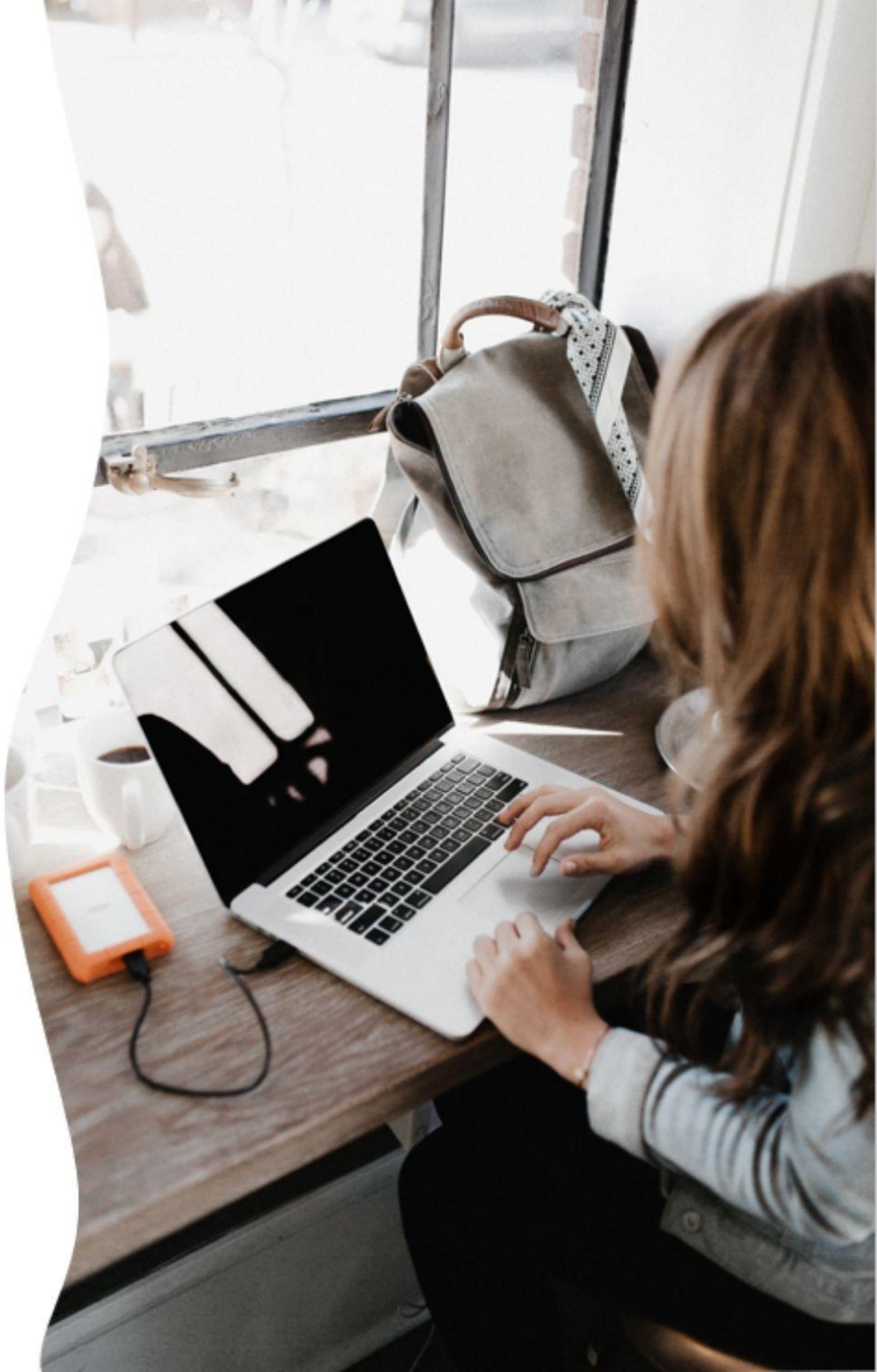
Miradore

A Preview of New Features in Miradore Management Suite 5.7.0



Miradore

What’s new in MMS 5.7.0

Asset management

- A new way to populate asset groups using a custom report
- An integration script for importing user data from Azure Active Directory

Patch management

- A new task for starting patching immediately
- A way to notify device users about patch installations
- Possibility to hide irrelevant patches in Miradore
- Exclude filters to automatic patch approval rules

Initial installation

- Initial installation from a network share now supports the use of HTTP packages

Security

- Two-factor authentication can now be enforced to all Miradore users
- Fixes to multiple non-critical security vulnerabilities in MMS and its components

New component versions

Miradore Management Suite server 5.7.0

Miradore Client for Windows 3.5.11

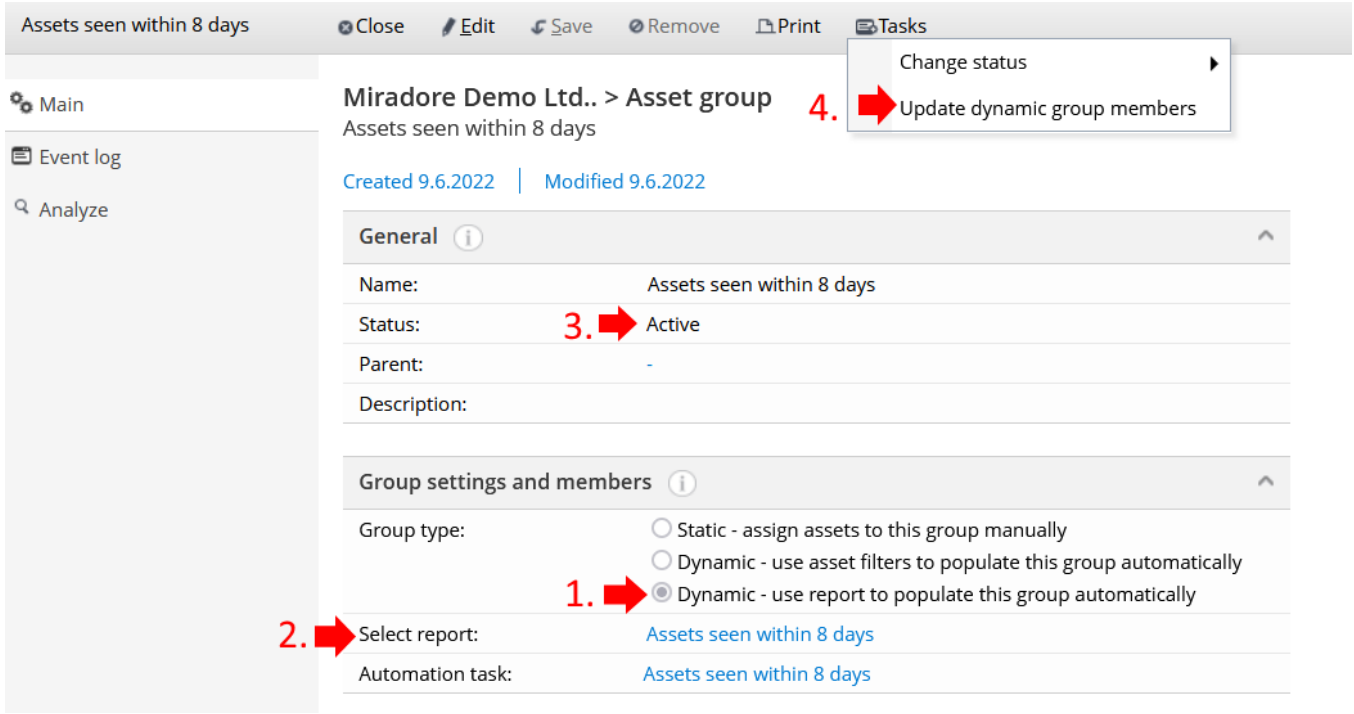
- Uses new libraries (OpenSSL 1.1.1m and cURL 7.82.0) which improves client security and robustness

SNMP scanner 2.4.0

- Supports TLS 1.2 in communication
- Requires .NET 4.7.2

A new way to populate asset groups

Miradore can now auto-populate asset group from a selected Report builder report listing assets.

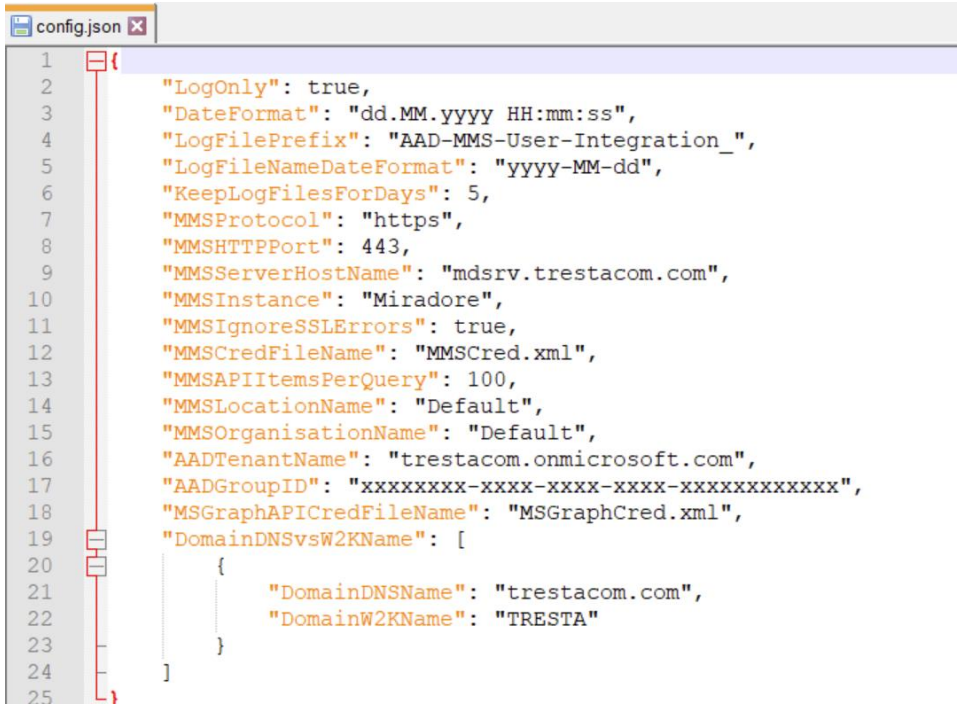


Azure AD integration script

It is now possible to import user data from Azure AD to MMS using a configurable script.

The provided script retrieves users that are members of a specified Azure AD group and creates them into Miradore.

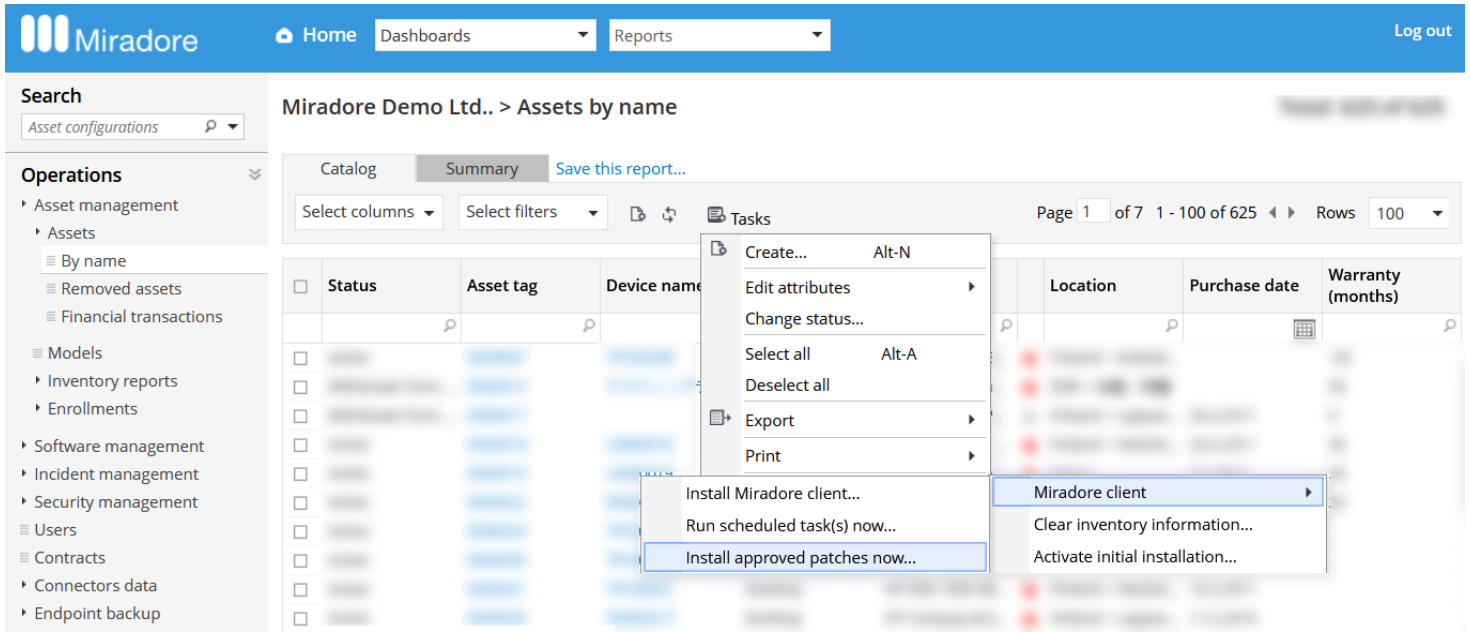
Any updates to the other user attributes (email, first name, last name, phone number, User ID) will be also replicated.



A way to start patching immediately

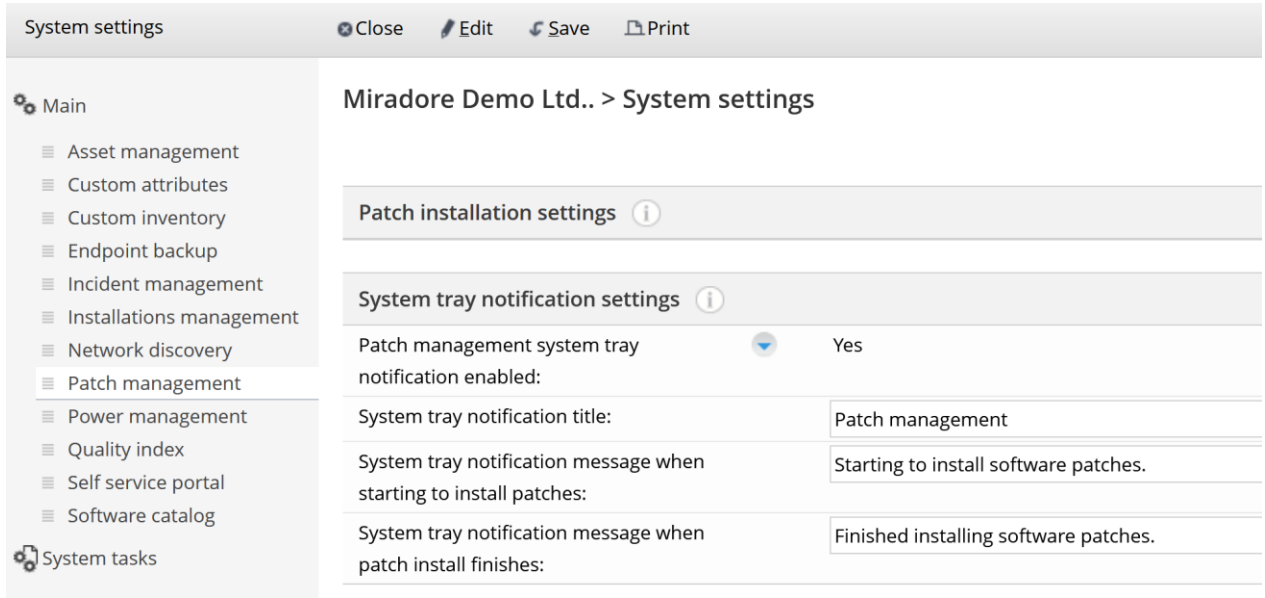
Patching can now be started immediately for selected devices from Miradore.

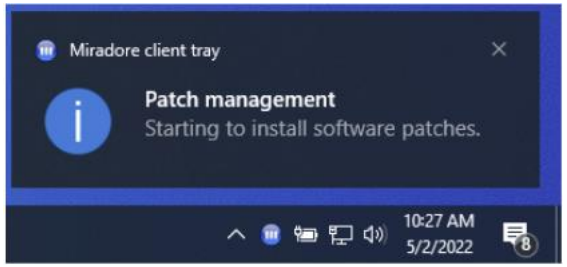
With this task, admins can take immediate action when devices are unoccupied or in urgent need of patching.

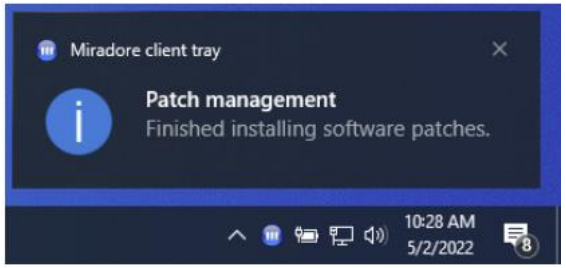


A way to notify users of patching

Miradore can now be configured to show a notification to user when patching is started and completed.



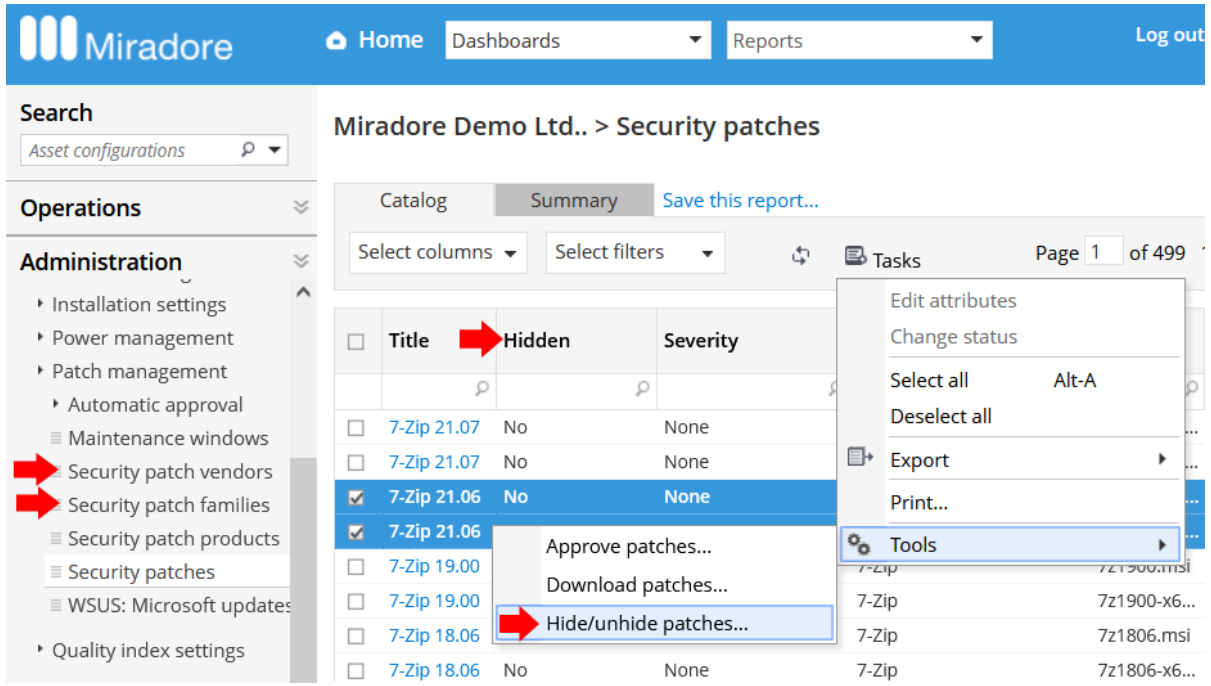




Possibility to hide patches

It is now possible to hide irrelevant patches in Miradore.

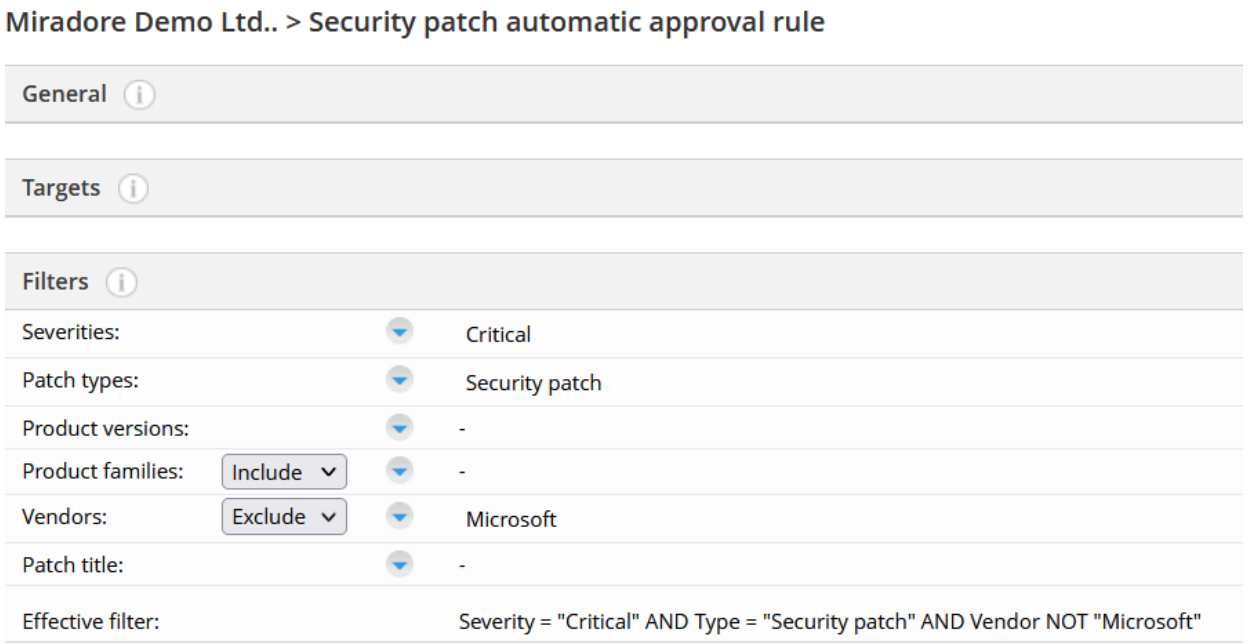
You can hide either selected patch(es), or patches from a certain vendor, or patches for a certain product family.



Exclude filters to patch approval rules

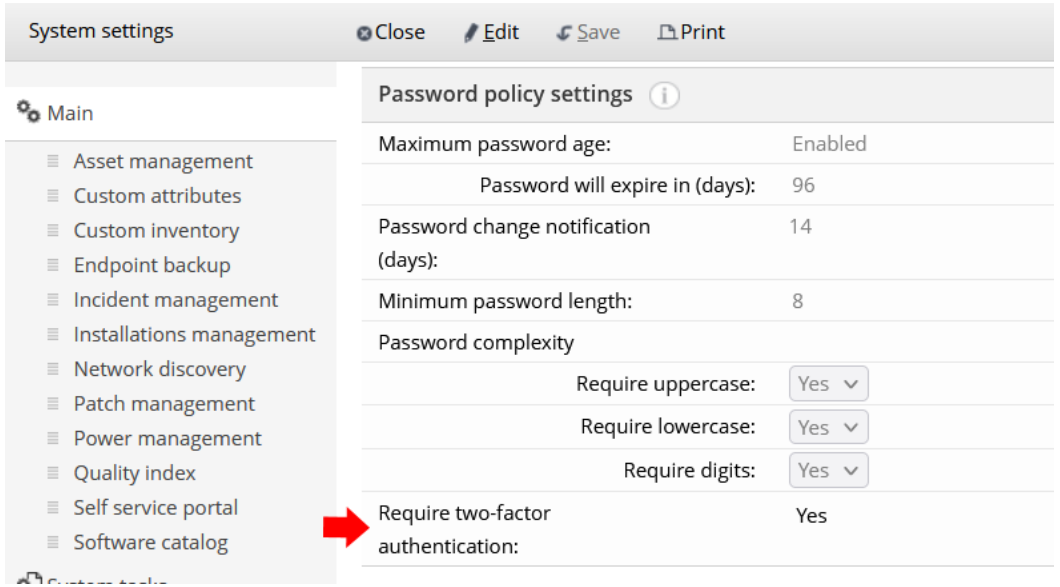
Now it is possible to use **Exclude** filters in the automatic patch approval rules.

This allows to build more advanced and accurate rules for processing the patch approvals.



Enforce 2FA for Miradore users

All Miradore users can now be forced to enable two-factor authentication for Miradore login.



Miradore

Other improvements

Description
It is now possible to add custom attributes with unlimited drop-down options for assets. Previously, the number of drop-down options was limited to 20.
Miradore’s Asset data import tool was improved to support custom asset attributes. See Product Guide for details.
Miradore MSP Console connector now replicates more detailed information about device's location (full location name) and operating system (full version and release ID) to the MSP Console.
Miradore Windows Client now stores the Client - Server connection settings before client upgrade. This ensures that the client can still connect to the MMS server with the previous settings in case the client would get faulty connection settings during the client upgrade.
Initial installation of Debian devices now allows to add extra files to the initial root file system (initrd).
Patch manager is now more robust as it restarts itself automatically at midnight if it stopped running due to an error situation.
Miradore Client now ensures that Miradore's tray process is running when it tries to show patching related reboot or postpone dialogs to device user.
Miradore installer now checks the existence of required certificates on the Patch manager host computer's certificate stores and notifies the user if any of them is missing.
Improvements and changes to the MMS web service API. See API documentation from the Product Guide for details.
For security reasons, Miradore now blocks the use of passwords that contain HTML markup like left-angle (<) and right-angle (>) brackets. Miradore users should be advised to change their password before upgrading to Miradore 5.7.0 if their password contains left-angle and right-angle brackets.

Miradore

Fixed bugs (1/2)

Description
If Miradore's SNMP scanner version 2.3 or earlier was installed in the environment, the installation of 3 Step IT connector accidentally removed the SNMP scanner. This bug has been fixed in the new SNMP scanner 2.4 version.
Data import using Microsoft Active Directory connector generated duplicate cost center items in Miradore if the cost centers already existed in Miradore but didn't have external identifiers configured. Miradore now checks the external identifiers during the data import and fills in the identifiers from the import data if they are missing from the cost center items in Miradore.
Miradore client installation failed on Ubuntu devices, because the "Release.key" file was missing from Miradore's Linux client repositories.
Initial installation failed with the error message "Failed to take ownership of TPM" when using Windows 11 ADK.
The disk space requirements check sometimes failed before operating system upgrade installations. Therefore, Miradore sometimes attempted to perform the OS upgrade although there wasn't enough free disk space left on the device.
The timeout limit for inventory data imports was increased from 15 minutes to 30 minutes. Previously, Miradore sometimes failed to process all the automatic patch approval rules within the 15 minutes and therefore some patches did not get approved as expected.
The installer of Miradore Management Suite did not disable PatchManager during Miradore upgrade and that could cause issues with the upgrade.
In certain circumstances, Miradore's Patch manager component started failing as it could not find the needed dll files.

Miradore

Fixed bugs (2/2)

Description
The list of available OS upgrade patches wasn't updated correctly in Miradore if an OS image, that superceded older operating systems, was removed from the media master installation point.
Sometimes the patch management reboot dialog was unnecessarily shown to device users.
Patch management client didn't handle http redirects correctly which could cause patch downloading directly from the Internet to fail during initial installation.
Fix to a vulnerability in Self-service portal that allowed a malicious user to gain unauthorized access to view device and user data. The vulnerability affects only Miradore Management Suite instances where the Self-service portal is enabled. The exposed information contains device name, device model, serial number, MAC address, warranty information and the device responsible person's name, organization, company name, location and possibly detailed location and cost center information. This fix is included in Miradore 5.6.0 Hotfix 1 package that was released in April 2022.
This version fixes some potential security vulnerabilities in Miradore Management Suite and its components. The vulnerabilities are non-critical and they were detected in a third-party security audit conducted recently. We highly recommend to upgrade any earlier versions of Miradore Management Suite as soon as possible although there isn't any known exploits of these vulnerabilities.
Fixed security vulnerabilities in the Command line tool.