Ivanti Neurons for Service Mapping Release Notes

V6.1.6 (September 2026)

This release delivers new features, enhancements, and bug fixes across Discovery, CMDB, Admin, and the Discovery Application and Agent. These updates automatically display upon upgrade and do not disrupt daily use for existing customers.

What's new

Service Mapping	Feature Enhancements
Discovery	• **AWS Account Name Support for Imports** Enhanced AWS imports to fetch and display the AWS Account Name wherever supported, alongside the existing Account ID. • **Cisco Wireless Controller managed Access Points** Added support to discover all Access Points managed by Cisco Wireless Controller devices. **Note:** The **MAC Address** must be configured as a correlator for the Access Point Blueprint to use this feature. • **Dell Device Warranty Lookup** Added support for Dell device warranty lookup through the TechDirect API. Users can configure their API credentials to automatically retrieve warranty details for discovered Dell devices in the CMDB. • **Meraki Serial Number Mapping** Added support to populate the Meraki device serial number in the **Serial Number** attribute, in addition to the existing **Device Serial Number** attribute.
CMDB	There are no new features and enhancements in this release.
Admin	• **Dell Warranty API Credentials** Added support to configure Dell TechDirect API credentials for retrieving warranty information for discovered Dell devices. • **Software Usage Report Version Column** Added a Version column to the Software Usage Report grid and Excel export. Users can now identify usage by software version directly in the report without manually cross-checking the Major Software configuration.
Discovery Application (v6.1.4032) and Discovery Agent (v6.1.126)	There are no new features and enhancements in this release.

Service Mapping	Feature Enhancements
Global Platform Changes	• **On-Demand Vulnerability Scanning** Added support for on-demand vulnerability scanning directly from CI Details. Users can also use the Process Vulnerability job to scan one or more selected CIs for vulnerabilities.

Fixes

These fixes automatically display upon upgrade and do not disrupt daily use for existing customers.

Service Mapping	Fix
Discovery	• **Handle Empty Host Name in Azure VM Import** Fixed Host Name mapping to use Computer Name when available, falling back to VM Name only when Computer Name is empty. • **Intune Import** Fixed an issue where Microsoft Intune imports did not retrieve all managed devices. • **Router Serial Number Discovery** Fixed an issue where router scans completed successfully but did not populate the Serial Number field on the discovered Router CI.
CMDB	• **Azure Virtual Machine Property Mapping** Fixed an issue where several Azure Virtual Machine properties were missing after Move to CMDB. Key properties and relationships are now correctly mapped to the resulting CI when available from Azure discovery.
Admin	• **Software Usage Total Used Time** Fixed an issue where the Software Usage summary report displayed only the latest session duration instead of the total usage time across all sessions in the selected reporting window.
Discovery Application (v6.1.4032) and Discovery Agent (v6.1.126)	**Discovery Application** • **Windows Scan with JEA Credentials** Fixed an issue with Windows scans using JEA-configured credentials, where certain commands did not use the configured JEA settings during the scan. **Discovery Agent** • **Software Usage Metrics Duplicate Submission** Fixed an issue where pending software usage metrics could be submitted multiple times after the Discovery Application became available and the agent restarted. • **Software Usage Process Tracking** Fixed an issue on macOS and Linux hosts where helper or companion processes could be incorrectly tracked as separate software usage instances, resulting in duplicate usage records.

Service Mapping	Fix
Global Platform Changes	• **Vulnerability Management CVE Grid Sorting** Fixed an issue where the checkbox column in the Vulnerability Management CVE grid could shrink after sorting by CVE ID.

Note: For Discovery Agent and Application, though this is not a mandatory update for v6.1.6, we recommend you update them as it may contain performance and security related updates.

Post-Release User Actions

1. Users should clear their browser cache before using Service Mapping after the release to ensure the application loads the latest content and resources.

2. Sign in to the **Service Mappings** web application.

3. Navigate to the **Admin portal** > **Client (Discovery)** page.

4. Click the update icon to update the application version **6.1.4032**.

Note: If the application does not update after you click **Update**, network restrictions can prevent the download. In this case, download and install the latest application version manually, or use the available manual update method.

To manually update the application, follow the below steps:

1. Stop the Virima Discovery Application.
2. Click the appUpdates_6.1.4032.zip link and download the update file on the Discovery Application machine.
3. Extract the downloaded **ZIP** file.
4. Replace the files in the installation directory with the extracted files, using the paths below:

File	Destination Path
DAClient.jar	C:\Program Files\Virima Discovery Application\
version.txt	C:\Program Files\Virima Discovery Application\
logback.xml	C:\Program Files\Virima Discovery Application\config\logback.xml
update.jar	C:\Program Files\Virima Discovery Application\

Note: Replace only the specified files in their respective destination folders. Do not replace the entire **Virima Discovery Application** folder or the **config** folder. Overwrite the existing files when prompted.

5. Start the Virima Discovery Application.