Docusnap 15

New Features, Changes, and Upgrade to Docusnap 15

TITLE	Docusnap 15
AUTHOR	Docusnap Consulting
DATE	9/7/2026
VERSION	1.1 | valid from 7. September 2026

TABLE OF CONTENTS

1. Introduction

With the release of Docusnap 15, several new features and changes are being introduced in Docusnap. This document is intended to give you an overview of these new features and changes. It also describes how to perform an upgrade to Docusnap 15.

New System Requirements

- **With Docusnap 15, at least a Microsoft SQL Server 2017 (Express) is required!**
- **In addition, the compatibility level of the Docusnap database must be set to at least "SQL Server 2017 (140)".**
  This can be configured using the SQL Management Studio:

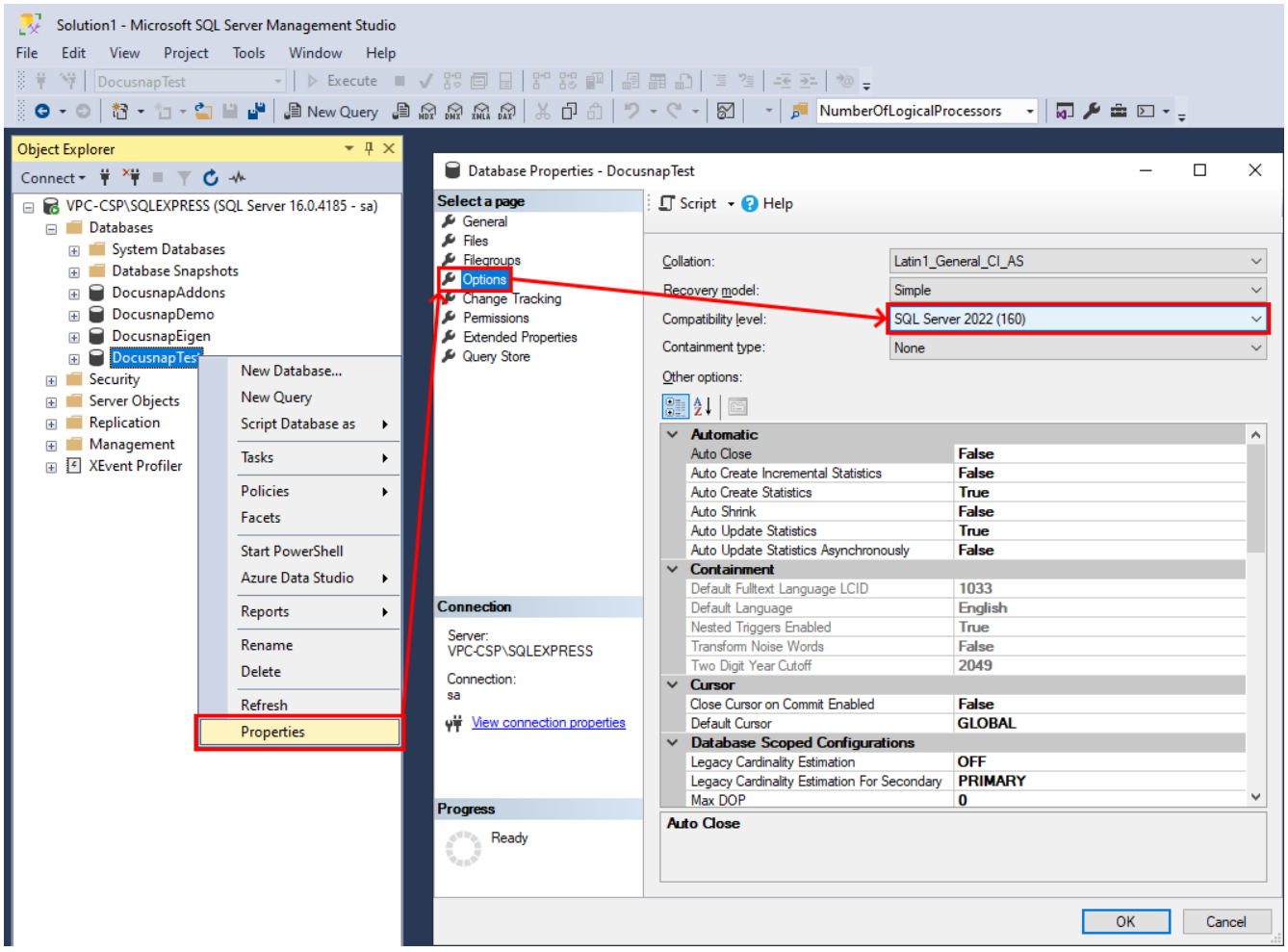

Figure 1 - Database compatibility level

New Features

- Proxmox Inventory
- Meraki Inventory

Changes

- Hyper-V
  - **Adjustment required!**
- Group Policies (GPO)
  - **No adjustment required!**
- Updates and changes to Discovery Services
  - **Adjustment required!**
- Linux – Docker Information
  - **No adjustment required!**
- Discovery Services – Components and Security Features
  - **Adjustment recommended (manual reinstallation)!**
- Removal of Legacy Wizards
  - Office 365
  - DFS Legacy

Performing the Upgrade

1. Docusnap 13 or 14 is installed
2. Active service contract / rental agreement in place
3. Start the upgrade on the Docusnap Server
   Download the installation file – run it – perform the installation
4. Adjust shortcuts using a central configuration file when the -UseConfig start parameter is used
5. The default program path to Docusnap.exe is now ...\Docusnap\...
6. Perform the database update
   First check when the last database backup was performed!
7. Replace the script files in use / adjust the share path
8. Update the DDS installations manually
   Component updates and new security measures.
9. Update the Docusnap client systems

2. Performing the Upgrade

An active service or rental contract is required for the free upgrade to Docusnap 15! Existing activation keys remain valid. You can download Docusnap 15 here.

An upgrade to Docusnap 15 is possible starting from Docusnap 13.

1. Start the upgrade on the server

In the first step, start the upgrade on the Docusnap Server. To do so, download the setup file from the homepage and run the installation.

2. Adjust the central configuration file (-UseConfig)

If you use a central configuration file with the -UseConfig parameter variant in the desktop shortcut, it must be adjusted. In the shortcut, update the paths for Target and Start in – the installation directory ...\Docusnap 14 becomes ...\Docusnap.

3. Check / perform the database backup

Before performing the database upgrade, you should perform a database backup if you have not already done so.

4. Perform the database upgrade

When you start Docusnap after the upgrade, Docusnap prompts you to update the database. If an active connection to the Docusnap database still exists, it will be displayed. Close all Docusnap client applications and then perform the database upgrade. The upgrade on the Docusnap Server is now complete.

5. Replace the script files in use / adjust the share path

If you perform inventory scans using one of the script variants, you must now replace them at their storage location. This replacement should be carried out after every update / upgrade of Docusnap.

When using one of the script variants, we generally recommend installing a Docusnap Discovery Service (DDS) at least on the system on which the Docusnap Server was also configured.

In the DDS settings, you can specify an additional directory for storing the inventory modules (script files). This ensures that the script files are automatically replaced during a Docusnap update and are therefore always up to date.

If you use the variant with deployment via the DDS, nothing needs to be adjusted!

Install and configure the DDS – How-To.
Here you will find a How-To that shows how to set up script-based inventory using Windows as an example.

6. Update the DDS installations

The Docusnap plugin files are automatically updated during a Docusnap update / upgrade. However, components such as NMAP or the NPCAP driver are not. For this reason, we recommend a complete update of all Docusnap Discovery Services.

For the complete update, the DDS setup must be run again on the respective systems. The DDS connections are re-established after the installation is completed.

You will find the setup programme in the Docusnap 15 installation directory, in the 'Setup' folder. Simply run the setup programme again. The existing installation will then be updated. You can use the -q parameter to run the installation in silent mode.

7. Updating the Docusnap Client Systems

Now you can also perform the upgrade on the remaining client systems. When Docusnap is started there, the message that an update is available appears automatically. -> Proceed as described!

As part of an update to Docusnap 14, installation on a network share was also supported by Docusnap. For client installations, it is recommended to share the installation over the network in the future. As a result, no client updates need to be performed for updates / upgrades.

The procedure is described in the Installation and Configuration How-To – Chapter 3!

3. Proxmox Inventory

The Proxmox inventory wizard requires the specification of any cluster node or a standalone node, along with a user including the realm (e.g. root@pam) that has read permissions on the cluster or node.

If a cluster is operated, specifying a single node is sufficient. Docusnap derives the entire cluster with all its nodes from it.

Inventory is collected via the manufacturer's API, which uses HTTPS on port 8006 and provides the following data:

- Cluster - Nodes, quorum, high availability (HA groups)
- Nodes - PVE version, hardware, storage, network
- VMs & Linux containers - CPU, RAM, network, snapshots
- Storage – Storage systems as well as Ceph with OSDs & pools
- Security – Firewall rules (cluster / node / VM)
- Users & Permissions – Authentication sources, groups, roles, permissions
- Backup – Backup jobs & replications between nodes

Reports are available at the cluster, node, VM, and container levels:

- Cluster – Cluster Overview: the entire cluster with its nodes and guests
- Nodes – Node Details (a single node), “Node Overall Report” (all nodes)
- Virtual Machines – VM Details (a single VM), “VM Overall Report” (all VMs)
- Linux Containers – Linux Container Details (a single container), Linux Container Overall Report (all)

To complete the documentation, the Proxmox nodes should still be added to the inventory as Linux systems!

4. Meraki

The Meraki inventory wizard requires the specification of a valid Meraki Cloud API key with appropriate read permissions for the Meraki organization.

The inventory is performed via the Meraki Cloud API (api.meraki.com) and uses HTTPS as well as port 443.

Reports are available at the Meraki organization level:

- Overview – Org Profile: organization, license, administration, security, networks, and devices.
- Device Inventory – All devices by product type and model: tags, serial, MAC, network, IP, status, firmware.
- Networks – Per network, the VLANs (subnet/gateway) and the active SSIDs with authentication.
- Licensing – License status and scope, as well as the active license items with expiration date.
- Security – Login/password rules, administrators (MFA), RADIUS, group policies, content filters.
- Switch Ports – Port profiles (Smartports) and the port assignment per switch.
- Cellular Gateways – Cellular gateways with status, carrier, SIM, and plan.

5. Hyper-V

The Hyper-V inventory has been redeveloped in Docusnap 15. The previous inventory wizard is retained for now as “Hyper-V Legacy”.

The Hyper-V inventory wizard requires the specification of the respective Hyper-V hosts (not clusters!) and the respective administrator on the Hyper-V host.

The other prerequisites remain unchanged compared to the legacy inventory.

New is the role-based detection of Hyper-V hosts based on the Windows inventory. This means that if Windows systems with the Hyper-V role installed have been inventoried, they can be displayed in the wizard.

Also new is the ability to perform a script-based inventory.

6. Group Policies (GPO)

In Docusnap 15, the technical settings of each group policy are now also captured. These include

- Status
- Computer configuration enabled
- User configuration enabled
- WMI filter path
- Creation date
- Modification date
- Owner

Furthermore, the policies are now also displayed in the Docusnap tree structure. This allows the policies to be analysed in detail and listed in reports.

At the Active Directory inventory and domain (AD-DS security) levels, the following GPO reports are available:

- Overview – all GPOs – curated table, one row per policy: Origin, status, scope.
- Details – all GPOs – each domain policy in full, one page per policy.
- Overview – linked GPOs – the same table, limited to those linked to the domain.
- Details – linked GPOs – the same level of detail, limited to the linked policies.
- Details – a single policy in full: links, delegation, settings.
- GPO security – examines all GPOs and displays GPOs with recorded security-related configuration
- Delegation deviations from the Microsoft standard; filed under ‘AD DS Security’

7. Linux – Docker information

The Linux scan in Docusnap 15 also detects Docker container hosts. If a Linux system is recognized as a Docker host, the Docker engine and the entire container landscape are included in the inventory. The following information can be found under the respective Linux system in the Docker branch:

- Overview & Engine
  - Docker, API, and Go versions, build time, and OS/architecture, as well as metrics: total containers/running/paused/stopped, images, Compose stacks, and networks.
- Containers
  - Name, image, status, and health status, creation time, restart policy, and container ID; additionally, for each container: ports, networks, and labels.
- Images
  - The container images present on the host.
- Networks
  - Driver (bridge, macvlan, host), scope, internal flag, IPv6, and network ID.
- Volumes
  - Name, driver, mount point, scope, creation time, and size.
- Compose stacks
  - Project name, working directory, config files, and health status.
- Components
  - Engine, containerd, runc, and docker-init, including version and Git commit.

8. Enhanced Protection

The enhanced protection in Docusnap 15 adds an additional layer of encryption for sensitive data in Docusnap. This includes:

- Docusnap database connection
  - With SQL authentication: the username and password
- Inventory information
  - Usernames and passwords of all inventory assistants
  - Private keys for Linux inventory
  - Entra ID app registration data

Enhanced protection is enabled in the Docusnap Server service configuration dialogue.

It is based on certificate encryption and thus extends the existing encryption. Once activated in the Docusnap Server service configuration dialogue, a certificate is installed on the system (Computer Store/LocalMachine).

If Docusnap is also used outside the Docusnap Server, the certificate must then be exported and installed on every system on which Docusnap is used. This also applies when launching Docusnap via a network share.

The certificate must then be exported and made available on every system on which Docusnap is started. This also applies when starting Docusnap from a network share.

The permissions for accessing the certificate/private key must be taken into account here. For certificates in the Computer Store, only SYSTEM and Administrators can access the private key by default and are therefore able to decrypt and use the data! There are two options for this:

a) Set private key permissions for a selected group of users (recommended: via an AD group), on each system where Docusnap is used.

b) Import the previously exported certificate, including the private key, specifically into the user certificate stores (CurrentUser) of the respective Docusnap users.

If the certificate is lost, all protected data must be re-entered. This includes scheduled jobs.

Without the certificate, no access to Docusnap is possible!

A database backup must be performed before activating the protection!

The certificate must be backed up! If it is lost, Docusnap can no longer be started.

The enhanced protection can only be disabled by losing data!

Customizings that modify or add input masks cannot be transferred to other Docusnap environments if the enhanced protection is activated.

9. New features and changes to the Discovery Services

If a Discovery Service (DDS) is installed with Docusnap 15, the components required for inventory scanning are no longer installed alongside it. The Docusnap Server loads these components only after registration.

This brings two advantages:

- The size of the installation package is significantly smaller – down from 400 MB to 75 MB.
- The components can be updated more easily.

With the previous installation method, NMAP was also placed in the Discovery Services installation directory, but was never updated. NMAP and the other inventory plugins are now stored exclusively under C:\ProgramData\Docusnap\Discovery\discovery – and are fully refreshed there with every update.

In addition, communication between the DDS and the Docusnap Server has been hardened.

We therefore recommend manually updating the Discovery Services so that the components are brought up to date and you benefit from the improved security.

You'll find the setup in the Docusnap 15 installation directory, in the Setup folder. Simply run it again – the existing installation will then be updated. The -q parameter lets you run the installation in silent mode.

10. Removal of Legacy Wizards

With Docusnap 15, the following outdated modules are discontinued:

- DFS – Legacy
- Office 365 – Legacy

If you are still running these inventory counts on a scheduled basis, you should delete these jobs and also remove the associated data from the tree structure.

Afterward, the current inventory counts should be scheduled: M365 and DFS.

LIST OF FIGURES

VERSION HISTORY

Date	Description
10. August 2026	Creation of the How-To
7. September 2026	Adjustment to enhanced protection – note added to the input forms