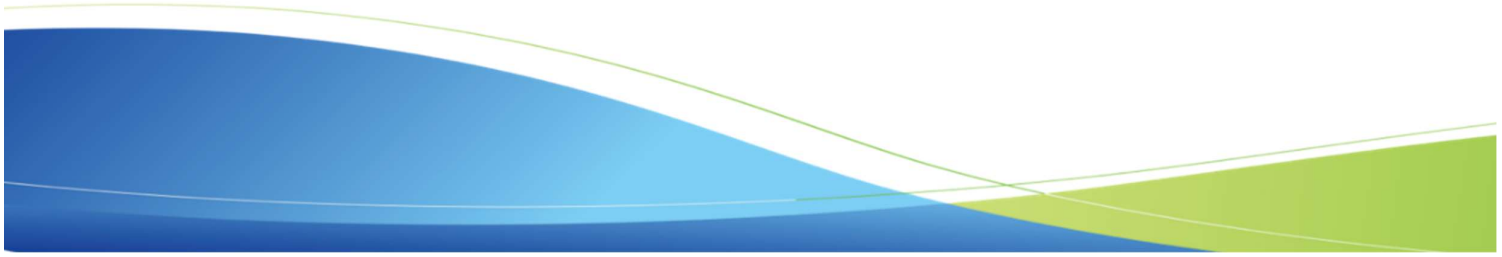


NovaGuard

Release Notes

Product Version	6.0.4ENR4
Document Version	002
Released On	July 28, 2025

ForeNova Technologies GmbH



Copyright Notice

Copyright © ForeNova Technologies B.V. 2025. All rights reserved.

Unless otherwise stated or authorized, ForeNova Technologies B.V. (hereinafter referred to as "ForeNova") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of ForeNova, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and ForeNova. Unless otherwise provided in the contract, ForeNova disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Contact Us

Hotline: +31 20 700 8895

ForeNova official website: www.forenova.com

About This Document

This document describes the release notes of NovaGuard.

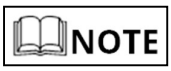
Intended Audience

This document is intended for:

- All Users

Note Icons

The following icons may appear in this article, and their descriptions are as follows.

Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Dec. 20, 2024	This is the first release of this document.

Contents

CONTENTS II

1 VERSION NAME 1

2 NEW FEATURES 2

2.1 ENHANCED SECURITY 2

2.1.1 Ransomware Decoy File Optimization 2

2.1.2 Malware Scan Optimization 3

2.1.3 Enhanced Protection Against Brute-Force Attacks 6

2.1.4 Vulnerability Detection Optimization 7

2.1.5 Windows Patching 9

2.2 OPTIMIZED MANAGER INSTALLATION AND DEPLOYMENT 10

2.2.1 Installation, Deployment, and Upgrade Restrictions 10

2.2.2 Installation Restrictions Lifted for SPs and Custom Packages 11

2.2.3 Progress Display for Deployment via OVA or OVA Image 11

2.2.4 Directory Space for Installation and Deployment 12

2.2.5 Configuration of Management IP Address 13

2.3 OPTIMIZED AGENT INSTALLATION AND DEPLOYMENT 15

2.3.1 Environment Check for Agent Installation and Deployment 15

2.3.2 Pre-installation Check for Linux Endpoints 17

2.3.3 Overwriting the Existing Agent on Linux Endpoints 17

2.3.4 Compatibility with OSes 18

2.3.5 Optimized Troubleshooting for Agent Installation 18

2.4 POLICY PUSH FROM NOVAXDR 19

2.5 NOVAGUARD (SAAS) FEATURE IMPROVEMENT 21

2.5.1 Agent Uninstallation After License Expiration 21

2.5.2 Cascade Deployment of NovaGuard (SaaS) 21

2.5.3 Custom Time Zone Settings 23

2.6 LAG AND STUTTERING REDUCTION 24

2.7 ADVANCED THREAT DETECTION AND RESPONSE 26

2.7.1 Upgrade Scenarios 26

2.7.2 Deployment Scenarios 27

2.7.3 License Edition Switch Scenarios 28

2.8 OPTIMIZED ENDPOINT MANAGEMENT 28

2.8.1 Optimization of Endpoint List and Endpoint Details 28

2.8.2 Move to This Group by IP Address (New Feature) 29

2.8.3 Display of Disk Usage 30

2.8.4 Removing Endpoints with Agent Disabled and Bypassed 31

2.9 EULA AND DPA OPTIMIZATION 32

2.10 NOVAGUARD AGENT UI UPDATE 33

2.11 O&M Operation Optimization 33
2.12 Installation by Endpoint Group 34
2.13 Domain Connectivity Tests 36
2.14 Optimization of Other Features 37

1 Version Name

The new version is NovaGuard 6.0.4ENR4, which can be upgraded as needed.

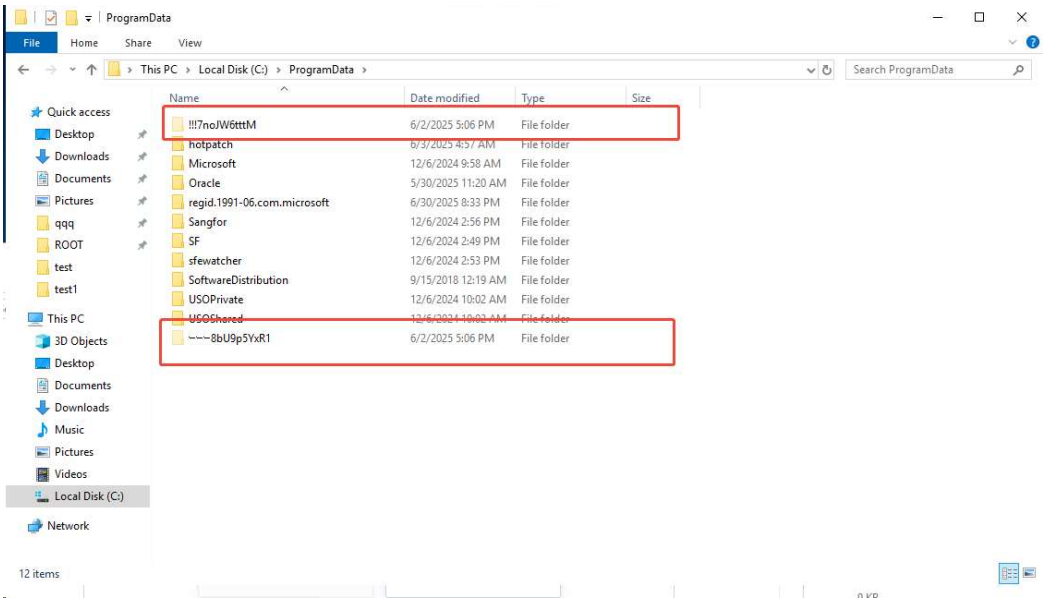
Please contact +31 20 700 8895 to obtain the update package.

2 New Features

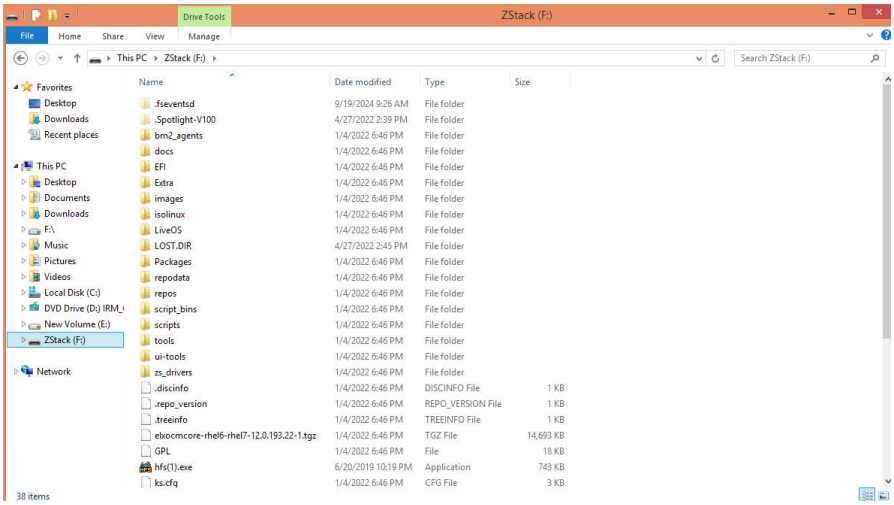
2.1 Enhanced Security

2.1.1 Ransomware Decoy File Optimization

1. Fixed the issue that the names generated for decoy files contained Chinese characters by replacing Chinese characters with other high-byte characters.



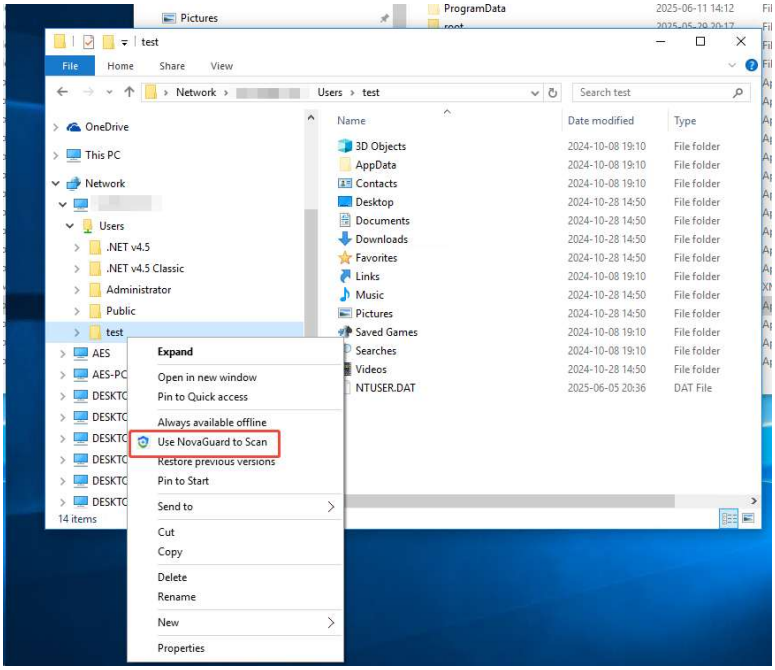
2. The following decoy files are no longer released to USB devices:



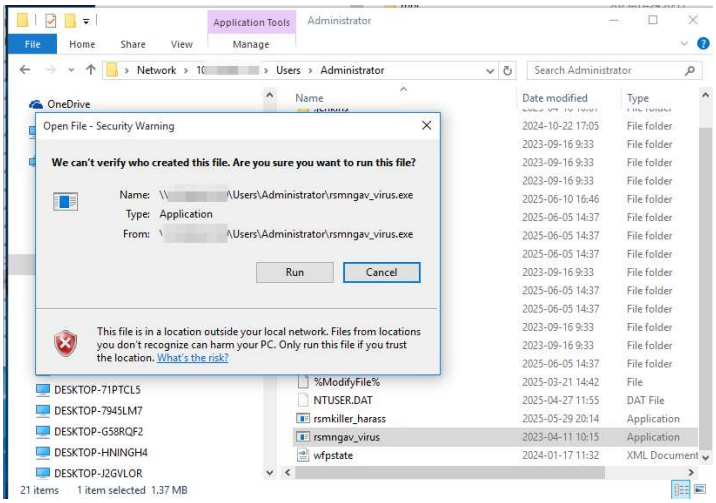
2.1.2 Malware Scan Optimization

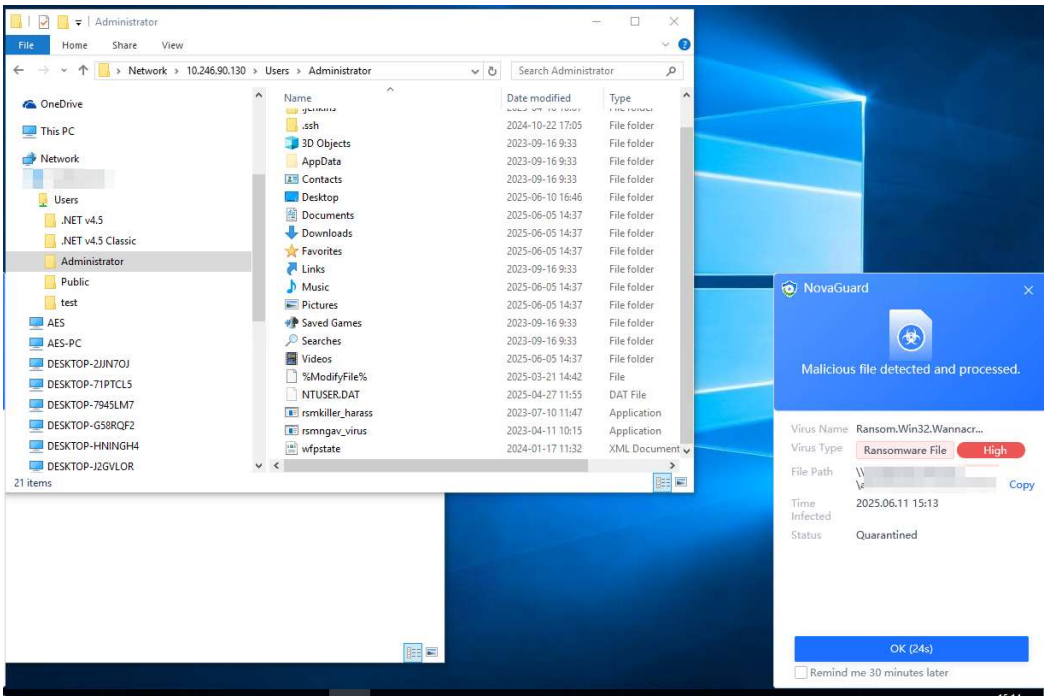
2.1.2.1 Malware Scan on SMB-Based Network Drives

1. Right-click a file on an SMB-based network drive and use NovaGuard to scan for viruses.



2. Realtime file protection against malicious processes is supported for SMB-based network drives.

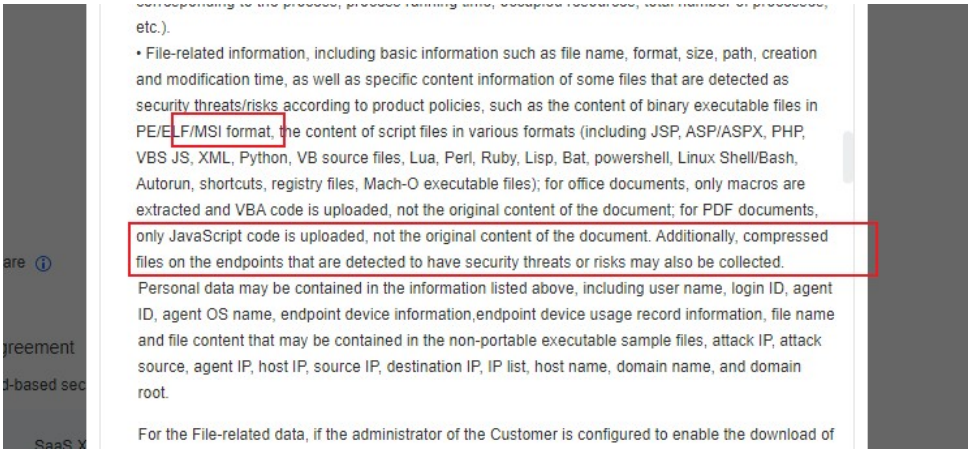




2.1.2.2 Reporting Unsigned MSI Files Smaller Than 50 MB to Cloud

Optimized the EULA and DPA agreements for the NovaGuard manager and agent.

NovaGuard Manager DPA:

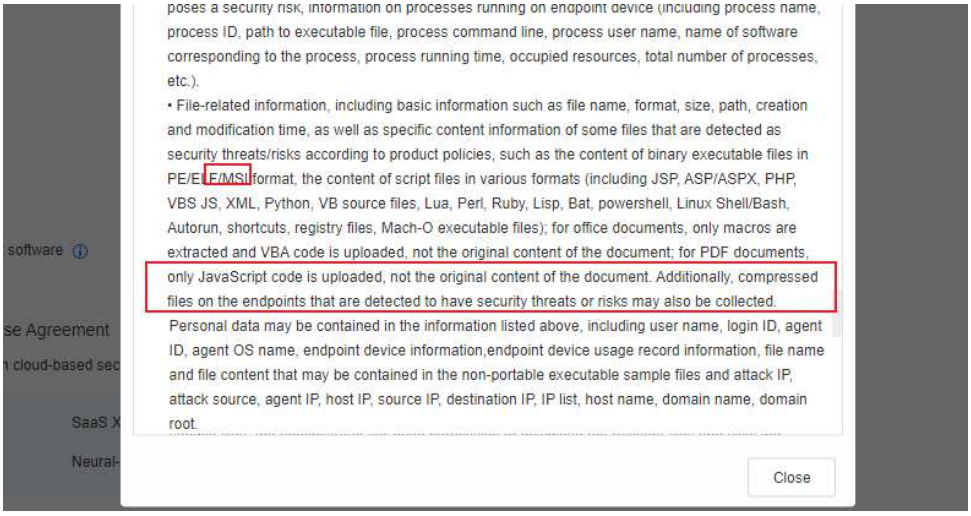


etc.).

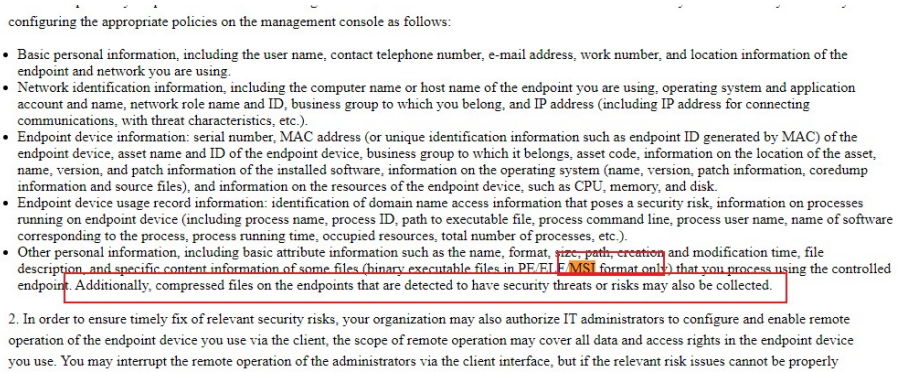
• File-related information, including basic information such as file name, format, size, path, creation and modification time, as well as specific content information of some files that are detected as security threats/risks according to product policies, such as the content of binary executable files in PE/ELF/MSI format, the content of script files in various formats (including JSP, ASP/ASPX, PHP, VBS JS, XML, Python, VB source files, Lua, Perl, Ruby, Lisp, Bat, powershell, Linux Shell/Bash, Autorun, shortcuts, registry files, Mach-O executable files); for office documents, only macros are extracted and VBA code is uploaded, not the original content of the document; for PDF documents, only JavaScript code is uploaded, not the original content of the document. Additionally, compressed files on the endpoints that are detected to have security threats or risks may also be collected.

Personal data may be contained in the information listed above, including user name, login ID, agent ID, agent OS name, endpoint device information,endpoint device usage record information, file name and file content that may be contained in the non-portable executable sample files, attack IP, attack source, agent IP, host IP, source IP, destination IP, IP list, host name, domain name, and domain root.

For the File-related data, if the administrator of the Customer is configured to enable the download of



NovaGuard Agent EULA:



configuring the appropriate policies on the management console as follows:

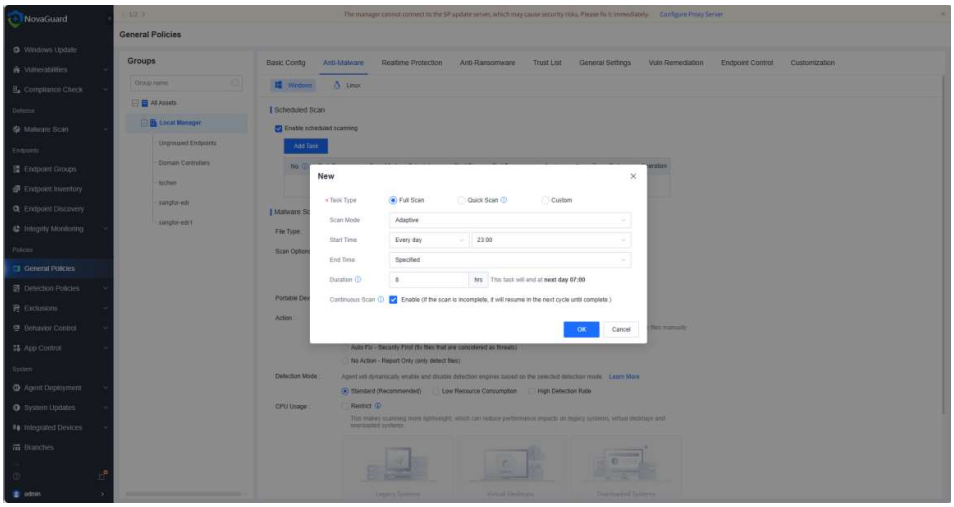
- Basic personal information, including the user name, contact telephone number, e-mail address, work number, and location information of the endpoint and network you are using.
- Network identification information, including the computer name or host name of the endpoint you are using, operating system and application account and name, network role name and ID, business group to which you belong, and IP address (including IP address for connecting communications, with threat characteristics, etc.).
- Endpoint device information: serial number, MAC address (or unique identification information such as endpoint ID generated by MAC) of the endpoint device, asset name and ID of the endpoint device, business group to which it belongs, asset code, information on the location of the asset, name, version, and patch information of the installed software, information on the operating system (name, version, patch information, coredump information and source files), and information on the resources of the endpoint device, such as CPU, memory, and disk.
- Endpoint device usage record information: identification of domain name access information that poses a security risk, information on processes running on endpoint device (including process name, process ID, path to executable file, process command line, process user name, name of software corresponding to the process, process running time, occupied resources, total number of processes, etc.).
- Other personal information, including basic attribute information such as the name, format, size, path, creation and modification time, file description, and specific content information of some files (binary executable files in PE/ELF/MSI format only) that you process using the controlled endpoint. Additionally, compressed files on the endpoints that are detected to have security threats or risks may also be collected.

2. In order to ensure timely fix of relevant security risks, your organization may also authorize IT administrators to configure and enable remote operation of the endpoint device you use via the client, the scope of remote operation may cover all data and access rights in the endpoint device you use. You may interrupt the remote operation of the administrators via the client interface, but if the relevant risk issues cannot be properly

2.1.2.3 Scheduled Scan Optimization

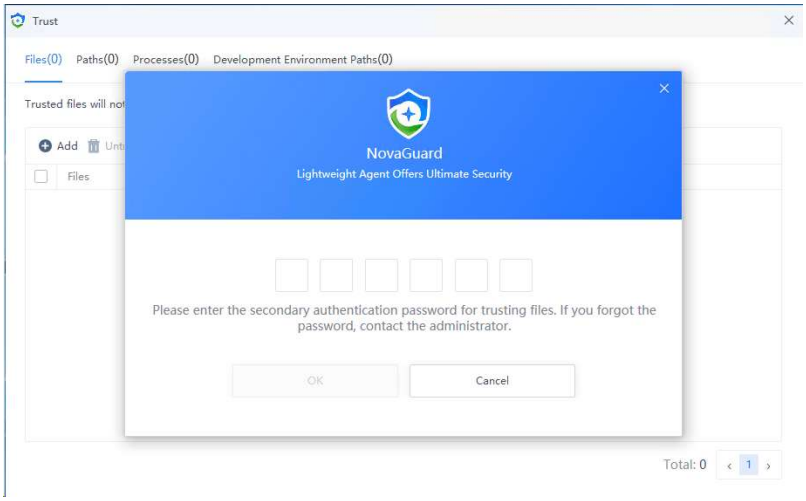
1. Enables **Continuous Scan** for full scan tasks by default, with the default scan end time extended to 8 hours after the original configured start time.

2. Supports scheduled scan tasks with **Continuous Scan** enabled for Windows endpoints. For example, a full scan task may be scheduled to start at 23:00 every day and end at 07:00 the next day. If the task is not complete during the period, it will be resumed in the next scan cycle (23:00-07:00).



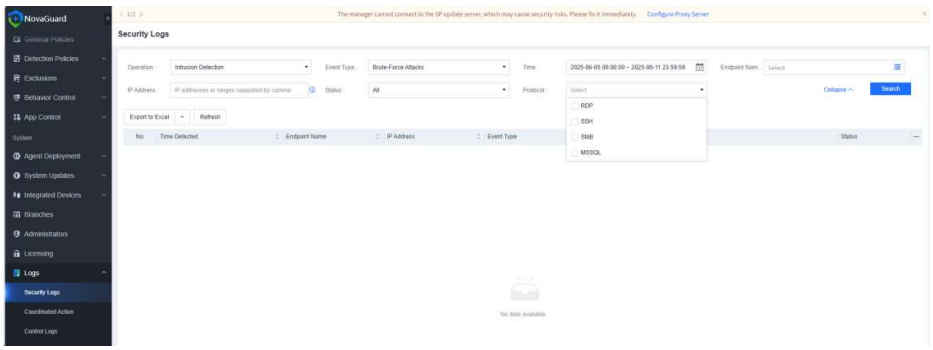
2.1.2.4 Trust Zone Password

After **Trust Zone Password** is enabled and a password is specified on the NovaGuard manager, the password is required for adding files to the **Trust** zone on servers and PCs.

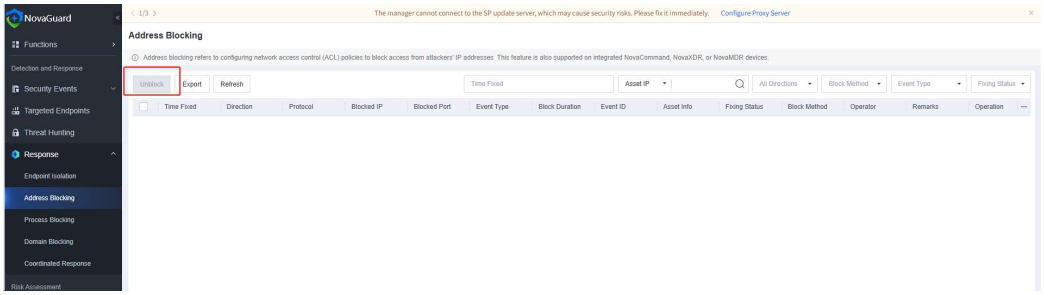


2.1.3 Enhanced Protection Against Brute-Force Attacks

Supports displaying protocols in the security logs for brute-force attacks and filtering the logs by protocol.

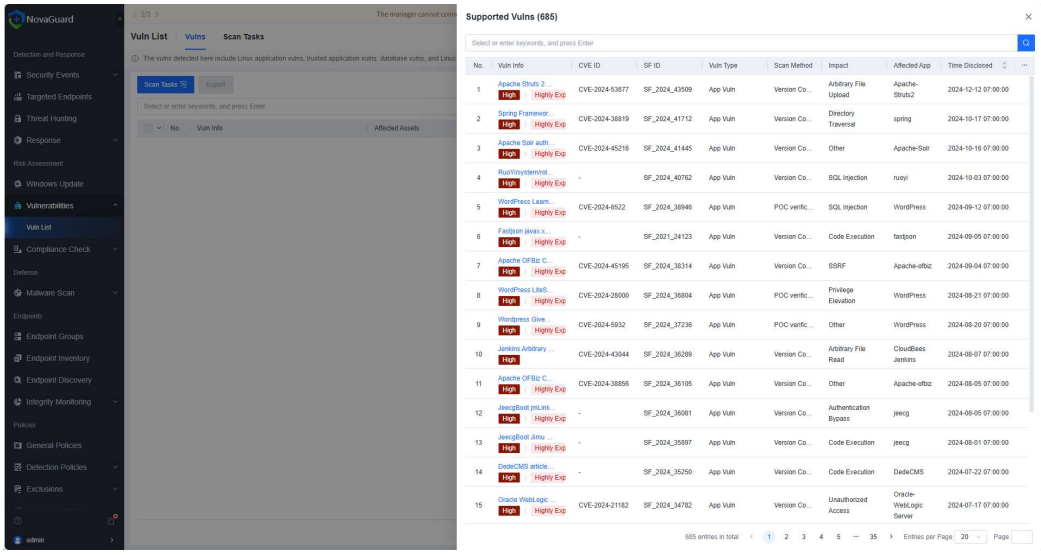


Supports bulk unblocking addresses.

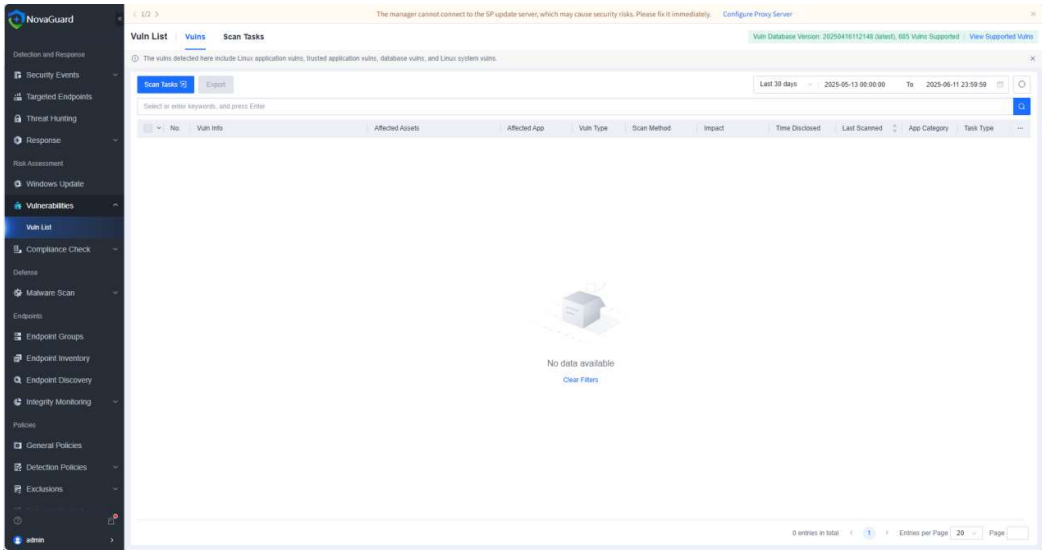


2.1.4 Vulnerability Detection Optimization

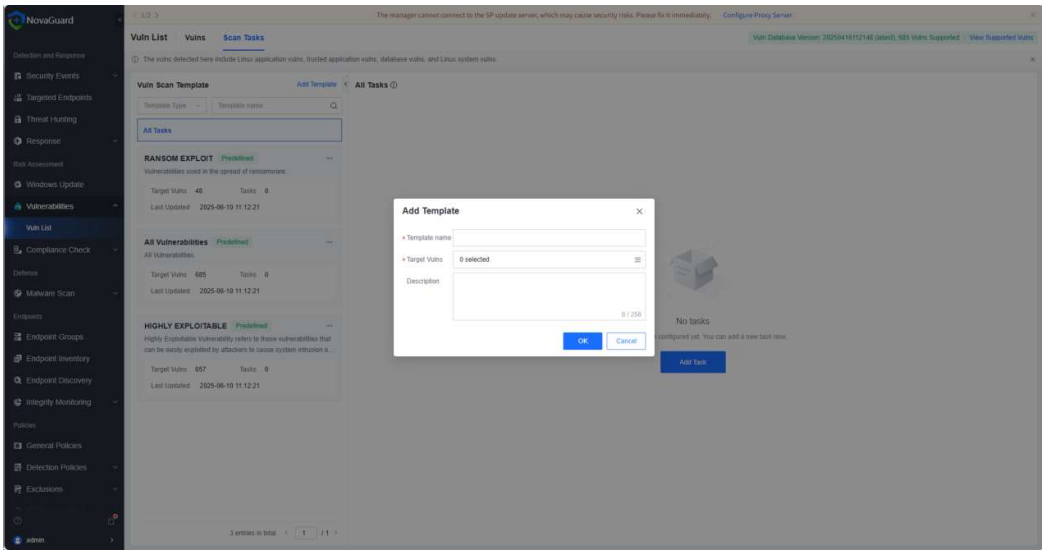
1. Optimized the vulnerability database and reduced the number of highly exploitable vulnerabilities that merit attention from over 15,000 to 685.



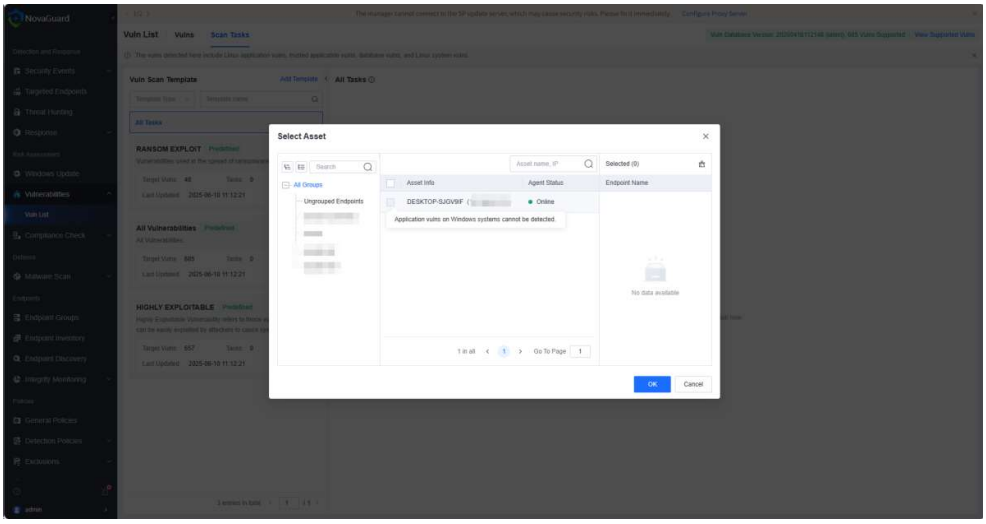
2. Optimized the information organization by separating Windows patches from vulnerabilities and moving the patches to the **Windows Update** module



3. Supports creating vulnerability scan tasks based on predefined or newly created templates. (Up to 64 templates can be created, and up to 64 tasks can be created using the same template.)

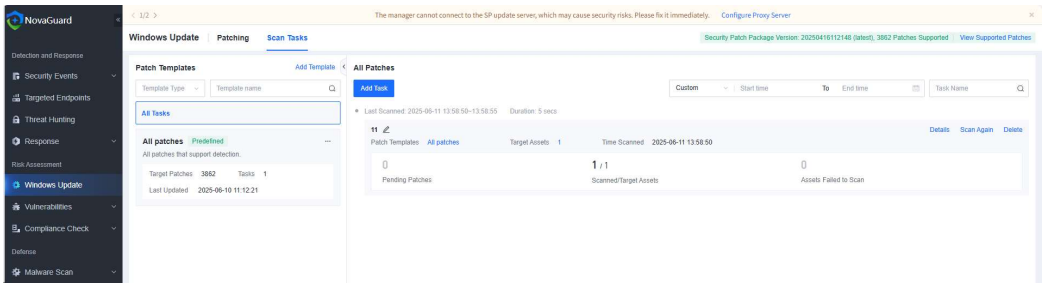


4. Grayed out unsupported endpoint types during vulnerability scan task creation. A tooltip is displayed when the cursor is hovered over an unsupported endpoint type.



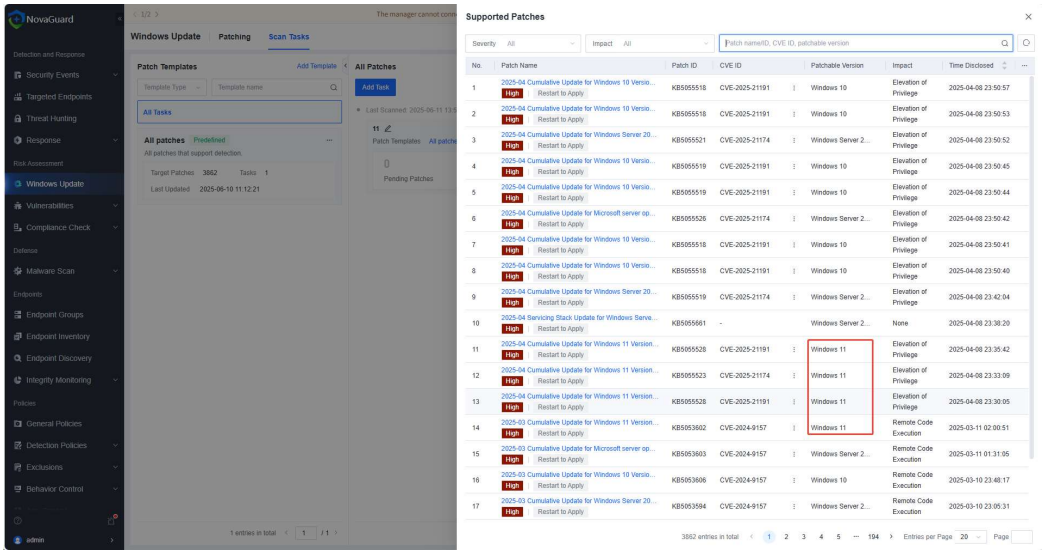
2.1.5 Windows Patching

1. Supports up to 3,862 Windows patches in a predefined template. Only Windows patches can be selected as target patches when a template is created.

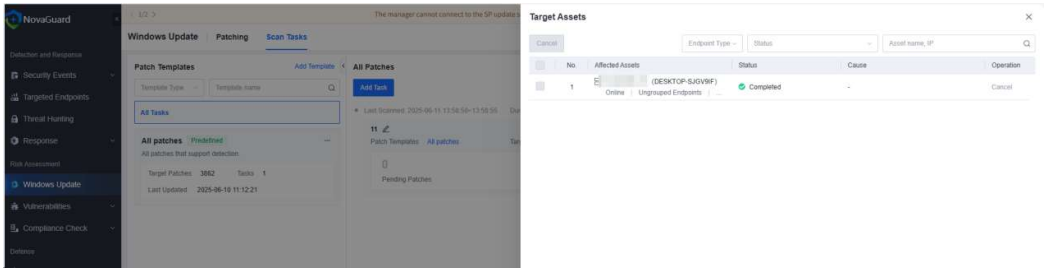


2. Supports viewing from the perspectives of patches and target assets, bulk sending of patches, and downloading a patch on the patch details page.

Go to **Risk Assessment** > **Windows Update** and click **View Supported Patches** in the upper right corner to view supported Windows 11 patches.



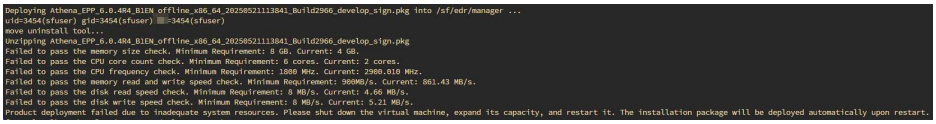
Patch detection is supported for Windows 11 systems.



2.2 Optimized Manager Installation and Deployment

2.2.1 Installation, Deployment, and Upgrade Restrictions

The following resources are required for deploying a manager that connects to 2,000 endpoints: at least 8 MB/s disk read/write speed, at least 6 CPU cores, over 8 GB memory, at least 1,800 MHz CPU clock speed, and at least 900 MB/s CPU read/write speed. Entries that do not meet the requirements will be displayed during deployment.



2.2.2 Installation Restrictions Lifted for SPs and Custom Packages

The administrator needs to install the pre-upgrade check package before performing the upgrade. If all SPs and custom packages are incorporated into NovaGuard 6.0.4ENR4 or later, the pre-upgrade check is passed, and the administrator can perform the upgrade. If some SPs and custom packages are not incorporated, the pre-upgrade check fails, and the administrator cannot perform the upgrade.

The unincorporated SPs and custom packages will be displayed after the pre-upgrade check is complete.

Pre-upgrade Check Report

Entity	Status (Passed: ✓, Not Passed: X)
The app protection policy check feature has been removed from the new version of Athena EPP. Check whether the policy data has been cleared from the RASP page.	✓
The disk encryption feature has been removed from the new version of Athena EPP. Check whether disks have been decrypted on the Endpoints > Endpoint Groups page.	✓
The anti web defacement policy check feature has been removed from the new version of Athena EPP. Check whether the policy data has been cleared from the Anti Web Defacement page.	✓
The remaining disk space is sufficient for the upgrade.	✓
The recommended maximum number of files that can be stored in the /tmp/ directory of the manager is 50000. The actual number of files stored in the /tmp/ directory is 100119119.	✓
The current product version includes custom packages or service packs that have not been incorporated into version 6.0.4ENR4_B1, and it cannot be directly upgraded to version 6.0.4ENR4_B1. Please contact Customer Service first. Packages not incorporated:	✗

2.2.3 Progress Display for Deployment via OVA or OVA Image

The administrator can view the progress when deploying the manager via an ISO or OVA image.

```
[   45.166621] MGR_INSTALL[889]: ############Start#############
[   45.167155] MGR_INSTALL[889]: Installing system software ...
[   45.167413] MGR_INSTALL[889]: ************End*************
[  105.181113] MGR_INSTALL[889]: ############Start#############
[  105.181735] MGR_INSTALL[889]: Starting pre-deployment ...
[  105.182173] MGR_INSTALL[889]: ************End*************
[  165.215800] MGR_INSTALL[889]: ############Start#############
[  165.216374] MGR_INSTALL[889]: Deploying the installation package, current progress: 10%
[  165.216792] MGR_INSTALL[889]: 2025-05-23 16:04:02 [step 1/5] Start unpacking the installation package.
[  165.217137] MGR_INSTALL[889]: ************End*************
[  225.229833] MGR_INSTALL[889]: ############Start#############
[  225.230436] MGR_INSTALL[889]: Deploying the installation package, current progress: 20%
[  225.230773] MGR_INSTALL[889]: 2025-05-23 16:05:41 [step 2/5] Start deploying the installation package.
[  225.231088] MGR_INSTALL[889]: ************End*************
[  285.244271] MGR_INSTALL[889]: ############Start#############
[  285.244808] MGR_INSTALL[889]: Deploying the installation package, current progress: 20%
[  285.245007] MGR_INSTALL[889]: 2025-05-23 16:05:41 [step 2/5] Start deploying the installation package.
[  285.245171] MGR_INSTALL[889]: ************End*************
[  347.165791] MGR_INSTALL[889]: ############Start#############
[  347.166541] MGR_INSTALL[889]: Deploying the installation package, current progress: 20%
[  347.166937] MGR_INSTALL[889]: 2025-05-23 16:05:41 [step 2/5] Start deploying the installation package.
[  347.167299] MGR_INSTALL[889]: ************End*************
[  407.188385] MGR_INSTALL[889]: ############Start#############
[  407.188936] MGR_INSTALL[889]: Deploying the installation package, current progress: 20%
[  407.189340] MGR_INSTALL[889]: 2025-05-23 16:05:41 [step 2/5] Start deploying the installation package.
[  407.189662] MGR_INSTALL[889]: ************End*************
[  467.203429] MGR_INSTALL[889]: ############Start#############
[  467.204173] MGR_INSTALL[889]: Deploying the installation package, current progress: 20%
[  467.204580] MGR_INSTALL[889]: 2025-05-23 16:05:41 [step 2/5] Start deploying the installation package.
[  467.204953] MGR_INSTALL[889]: ************End*************
[  527.215481] MGR_INSTALL[889]: ############Start#############
[  527.216272] MGR_INSTALL[889]: Deploying the installation package, current progress: 50%
[  527.216729] MGR_INSTALL[889]: 2025-05-23 16:10:42 [step 3/5] Start deploying the virus rule database.
[  527.217058] MGR_INSTALL[889]: ************End*************
[  560.142178] ip_local_port_range: prefer different parity for start/end values.
[  587.229592] MGR_INSTALL[889]: ############Start#############
[  587.230352] MGR_INSTALL[889]: Deploying the installation package, current progress: 90%
[  587.230767] MGR_INSTALL[889]: 2025-05-23 16:11:48 [step 5/5] Start the relevant business services of the management platform.
[  587.238245] MGR_INSTALL[889]: ************End*************
[  647.253769] MGR_INSTALL[889]: ############Start#############
[  647.258299] MGR_INSTALL[889]: Deploying the installation package, current progress: 90%
[  647.262681] MGR_INSTALL[889]: 2025-05-23 16:11:48 [step 5/5] Start the relevant business services of the management platform.
[  647.266518] MGR_INSTALL[889]: ************End*************
[  707.299138] MGR_INSTALL[889]: ############Start#############
[  707.303439] MGR_INSTALL[889]: Deploying the installation package, current progress: 100%
[  707.307291] MGR_INSTALL[889]: 2025-05-23 16:14:03 Deploy successful!!!
[  707.311799] MGR_INSTALL[889]: ************End*************
```

2.2.4 Directory Space for Installation and Deployment

The manager can be installed or upgraded successfully as long as the available space of the /tmp directory is over 300 MB. If the space is insufficient for installing or upgrading the manager, a prompt will appear.

Installation:

```
[root@beauty-mgr home]# ./manager_deploy_6.0.2.sh aES6.0.2R4_B1_offline_x86_64_20250611115306_Build17699_develop_sign.pkg 0.0.0.
0
cmd (firewall-cmd --version) result is 0.6.3
Firewalld ver ok
check disk size...
The mount point of /tmp/ is /tmp, failed to pass the disk size check. Minimum Requirement: 0.3GB. Current: 0.2GB.
The mount point of /data/, /sf/ and /ac/ is /, failed to pass the disk size check. Minimum Requirement: 26.2GB. Current: 18.1GB.
[root@beauty-mgr home]# sudo umount /tmp
[root@beauty-mgr home]# sudo mount -t tmpfs -o size=350M tmpfs /tmp
[root@beauty-mgr home]# ./manager_deploy_6.0.2.sh aES6.0.2R4_B1_offline_x86_64_20250611115306_Build17699_develop_sign.pkg 0.0.0.
0
cmd (firewall-cmd --version) result is 0.6.3
Firewalld ver ok
check disk size...
The mount point of /data/, /sf/ and /ac/ is /, failed to pass the disk size check. Minimum Requirement: 26.2GB. Current: 18.1GB.
[root@beauty-mgr home]# df -h
Filesystem              Size  Used Avail Use% Mounted on
devtmpfs                7.8G     0  7.8G   0% /dev
tmpfs                   7.8G     0  7.8G   0% /dev/shm
tmpfs                   7.8G  9.6M  7.8G   1% /run
tmpfs                   7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/mapper/centos-root   50G   32G   19G  64% /
/dev/vda1               1014M  171M  844M  17% /boot
/dev/mapper/centos-home  241G  5.3G  236G   3% /home
tmpfs                   1.6G     0  1.6G   0% /run/user/0
tmpfs                   350M  4.0K  350M   1% /tmp
[root@beauty-mgr home]#
```

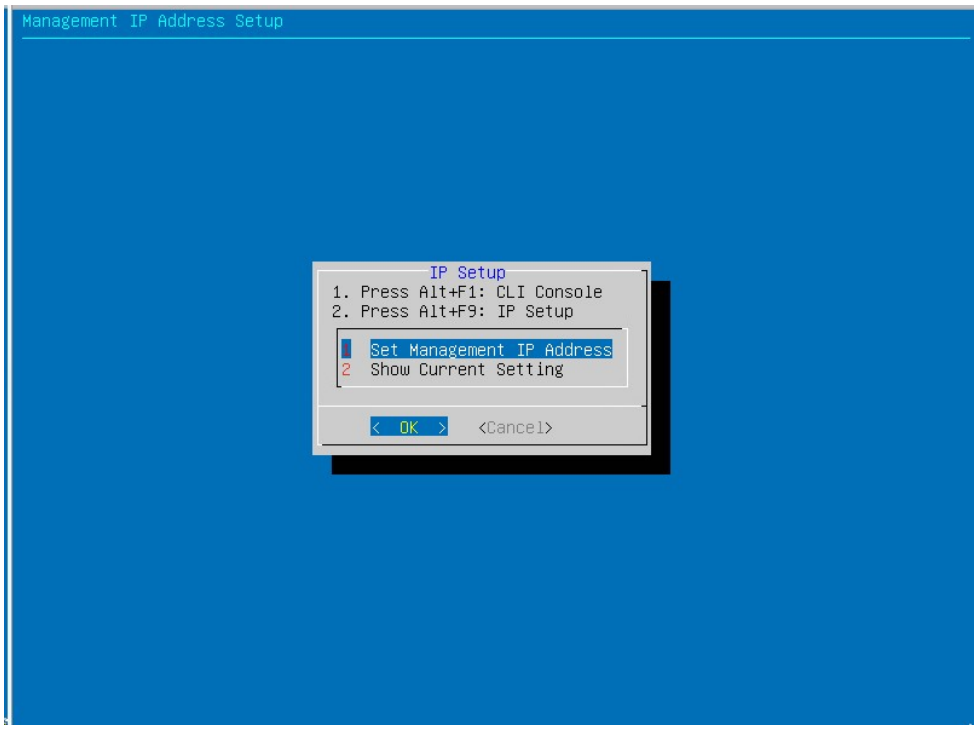
Upgrade:

Pre-upgrade Check Report

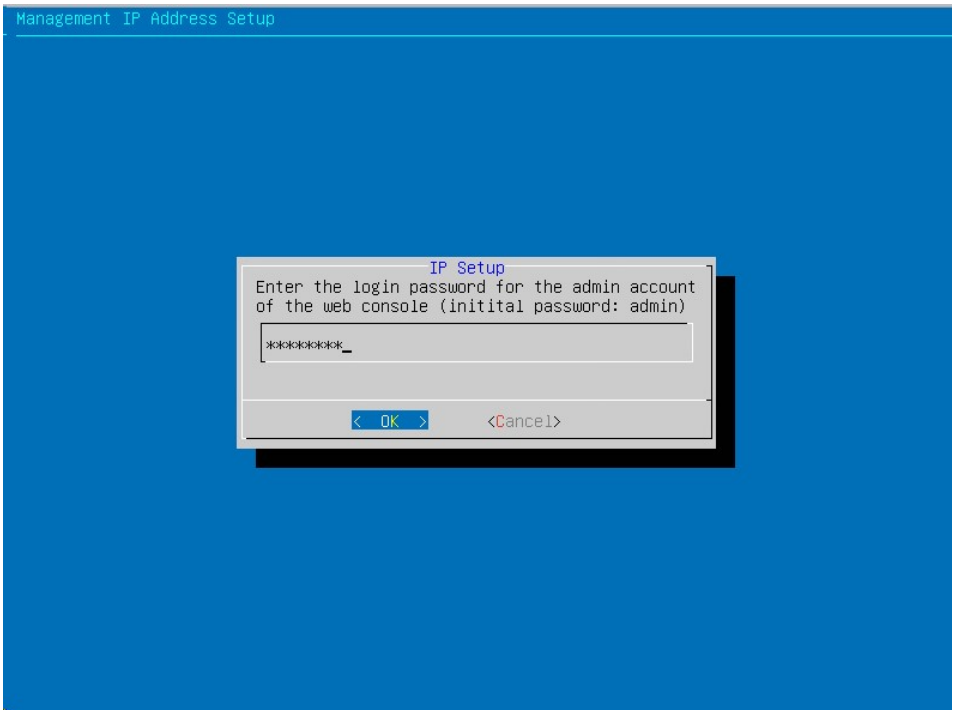
Entity	Status (Passed: ✓, Not Passed: ✗)
The app protection policy check feature has been removed from the new version of Athena EPP. Check whether the policy data has been cleared from the RASP page.	✓
The disk encryption feature has been removed from the new version of Athena EPP. Check whether disks have been decrypted on the Endpoints > Endpoint Groups page.	✓
The anti web defacement policy check feature has been removed from the new version of Athena EPP. Check whether the policy data has been cleared from the Anti Web Defacement page.	✓
For the disk partition mounted to the directory "/tmp", at least 1.99 GB of remaining space is required, and the remaining space is 0.19 GB.	✗
The recommended maximum number of files that can be stored in the /tmp/ directory of the manager is 50000. The actual number of files stored in the /tmp/ directory is 2030882.	✓
The current product version includes custom packages or service packs that have not been incorporated into version 6.0.4ENR4_B1, and it cannot be directly upgraded to version 6.0.4ENR4_B1. Please contact Customer Service first. Packages not incorporated: TD-2024010200277-5410115, EDR-2024103109-1999011.	✗

2.2.5 Configuration of Management IP Address

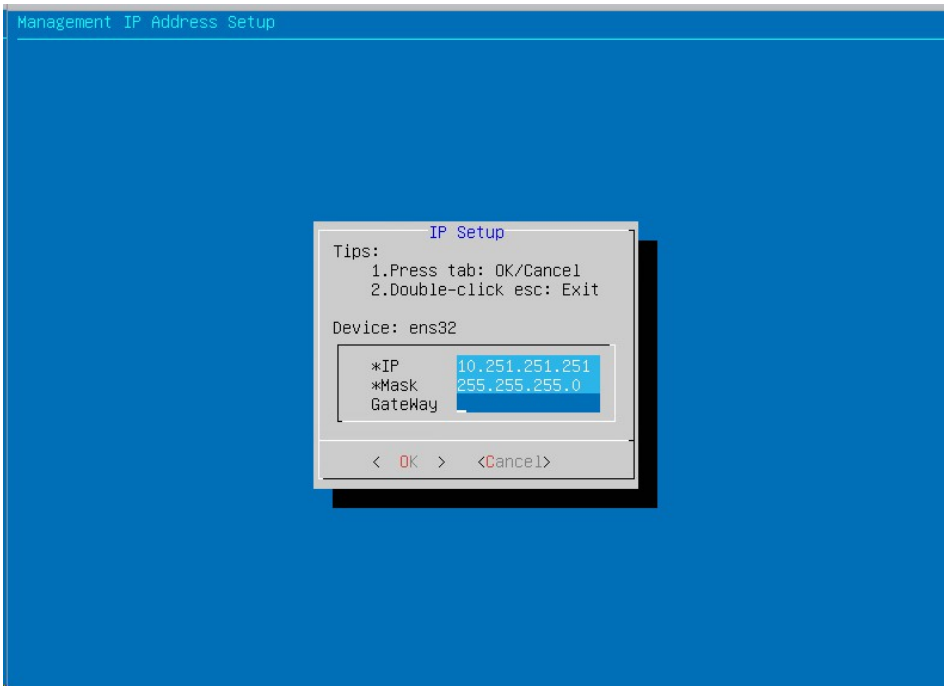
After the manager is deployed via an OVA or ISO image, the **IP Setup** dialog box appears. The administrator can click **Show Current Setting** to view the current management IP address or click **Set Management IP Address** to configure it.



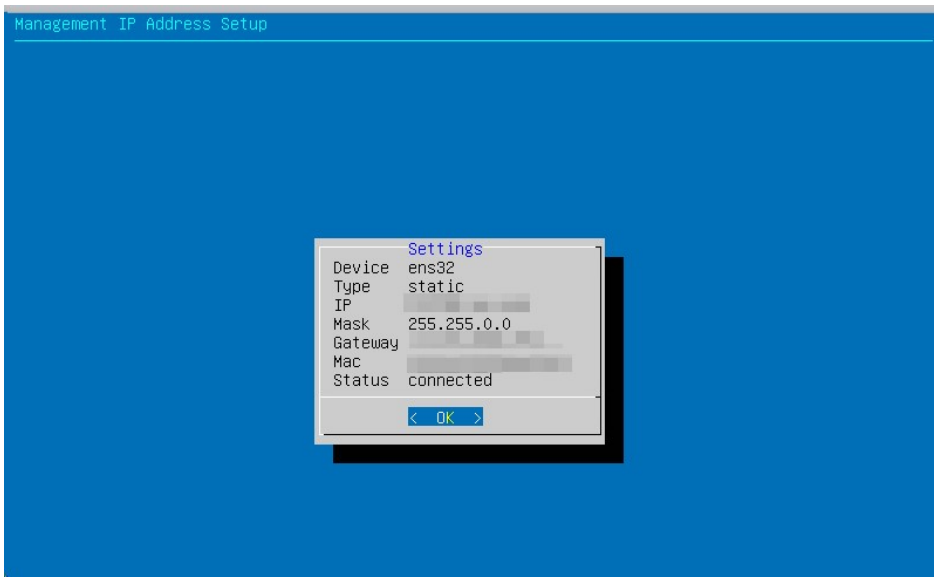
To configure the management IP address, enter the front-end admin password first.



Specify the management IP address and gateway address.



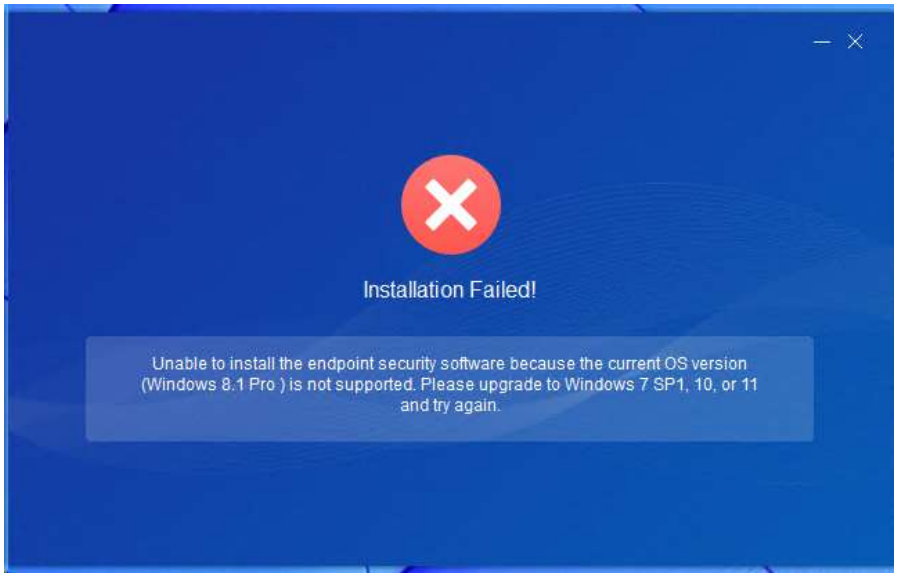
In the **Settings** dialog box, view the management interface, interface status, IP address, MAC address, and gateway address.

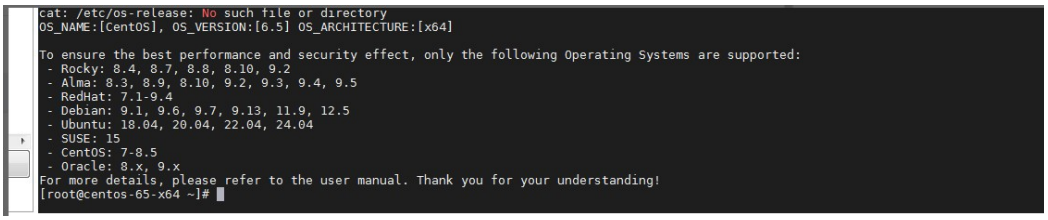


2.3 Optimized Agent Installation and Deployment

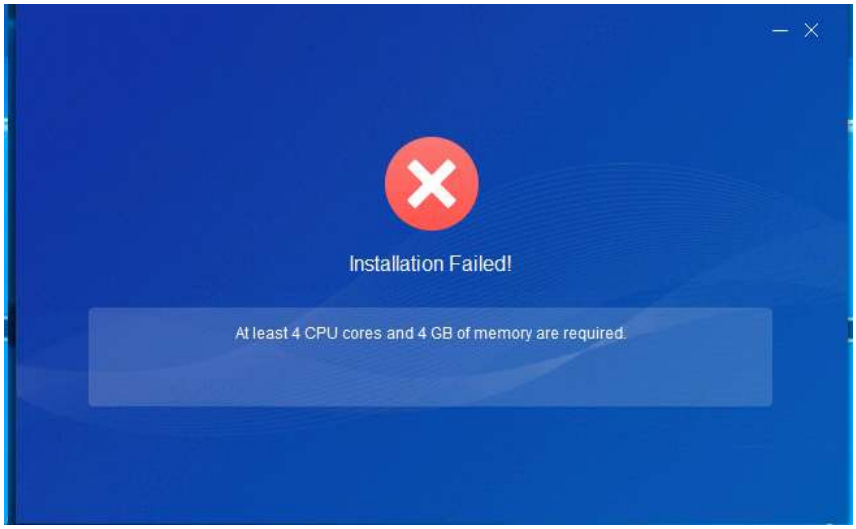
2.3.1 Environment Check for Agent Installation and Deployment

1. The Installation Failed message is displayed when installing the agent on Linux and Windows endpoints with incompatible OS versions.

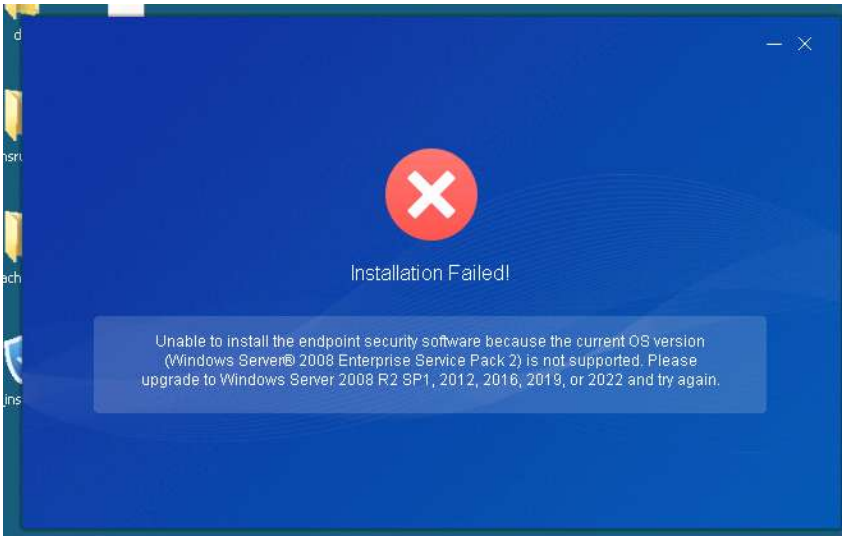




2. The Installation Failed message is displayed when installing the agent on Linux and Windows endpoints that do not meet resource requirements (at least 4 CPU cores and 4 GB of memory).

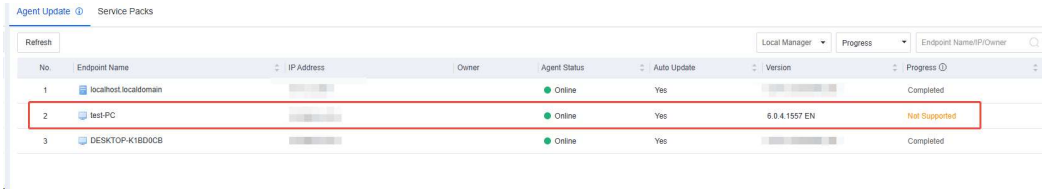


3. The Installation Failed message is displayed when installing the agent on Windows 7 and Windows Server 2008 R2 endpoints without the SHA256 patch.



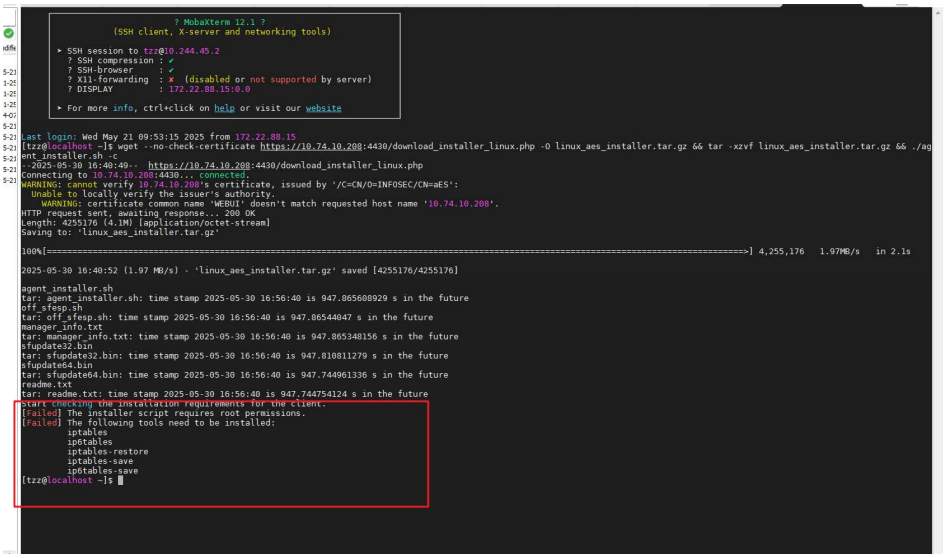
4. An unsupported upgrade message is displayed for Linux and Windows

endpoints with OS versions incompatible with the upgraded manager.



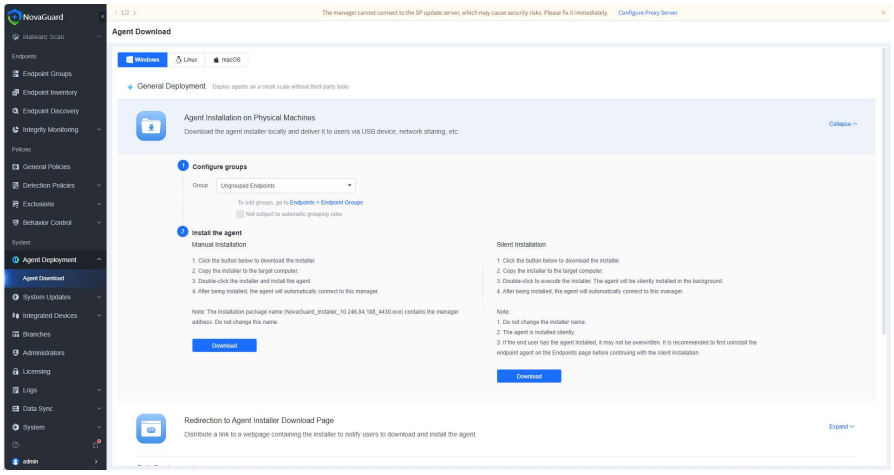
2.3.2 Pre-installation Check for Linux Endpoints

When the pre-installation check fails on a Linux endpoint, the issues will be displayed. The administrator can install the agent on the endpoint successfully after fixing the issues.



2.3.3 Overwriting the Existing Agent on Linux Endpoints

The administrator can copy and execute the command to install the agent on Linux endpoints that already have the agent installed. The existing agent will be overwritten.



2.3.4 Compatibility with OSes

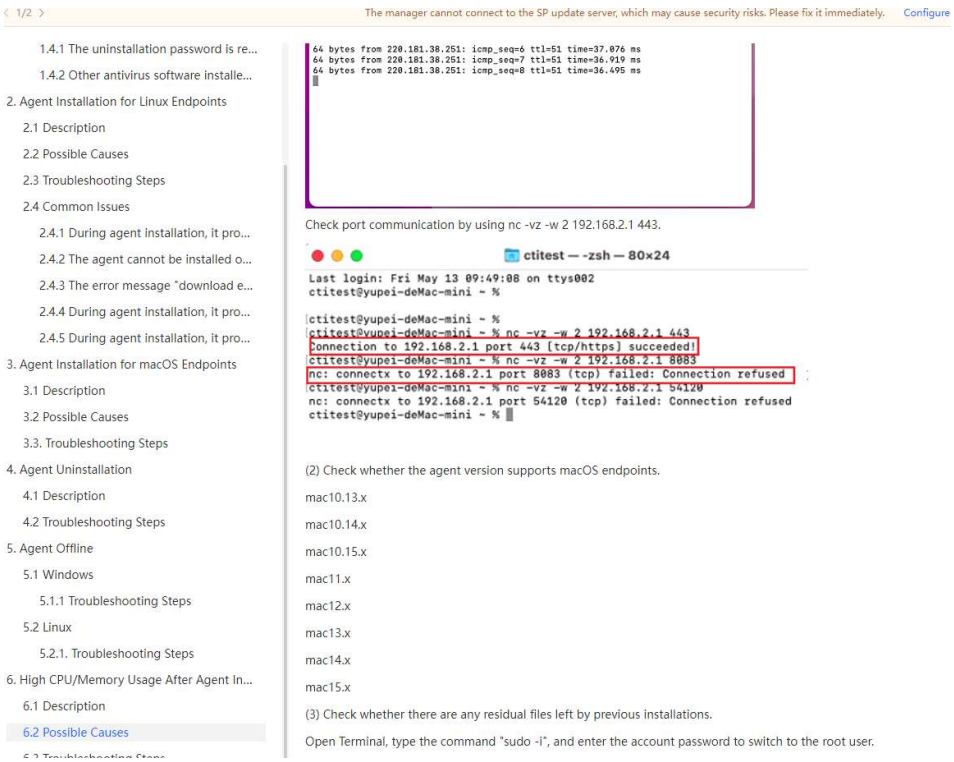
1. Supports more Linux systems. For details, see the table below.

6.0.4ENR4-Com
patible Systems.:

2. Supports more macOS systems, including macOS 10.13.x, 10.14.x, 10.15.x, 11.x, 12.x, 13.x, 14.x, and 15.x.

2.3.5 Optimized Troubleshooting for Agent Installation

1. The troubleshooting manual is given in **Troubleshooting** > **Agent FAQ** on the manager.



2. The specific causes are displayed when installation fails on Windows endpoints.

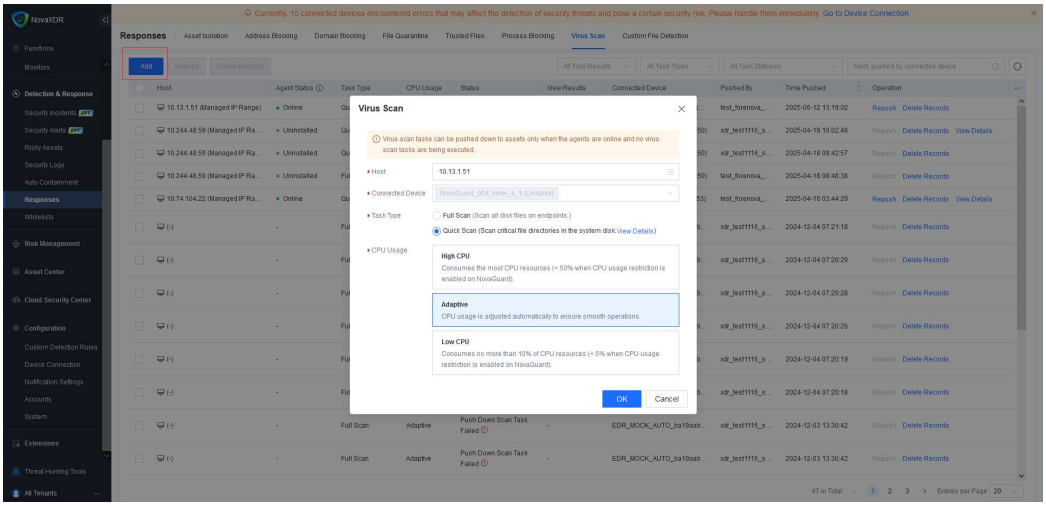


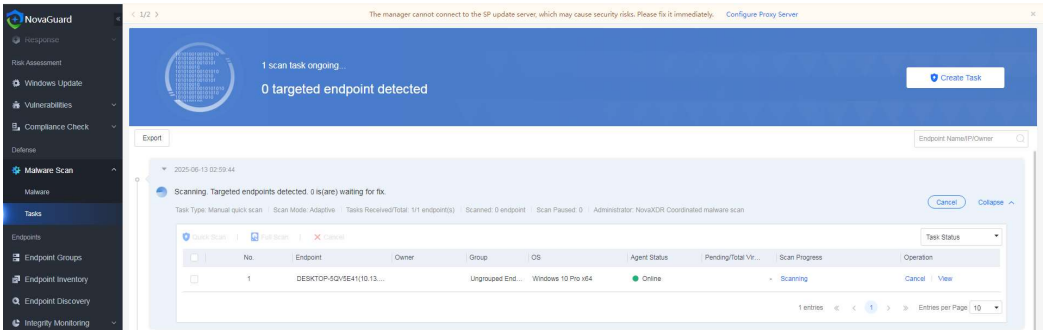
2.4 Policy Push from NovaXDR

After NovaGuard is integrated with NovaXDR, NovaGuard will report malicious files to NovaXDR. The administrator can push custom malware scan tasks, and IOC policies from NovaXDR to the NovaGuard agent. The procedure is as

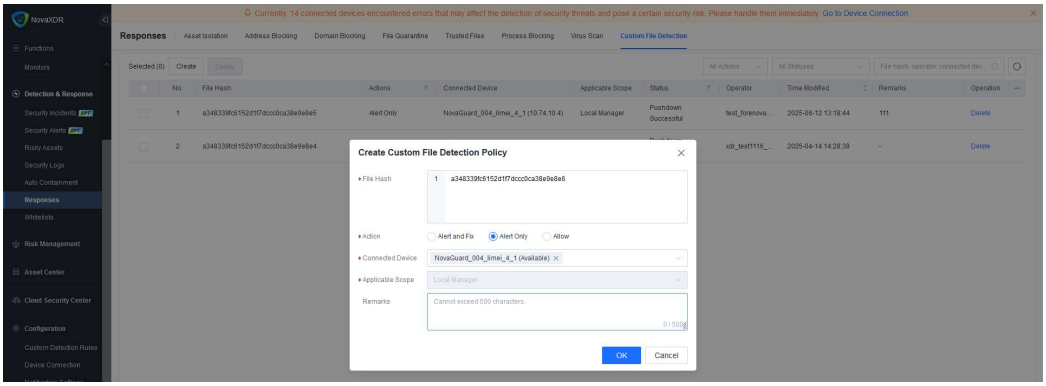
follows:

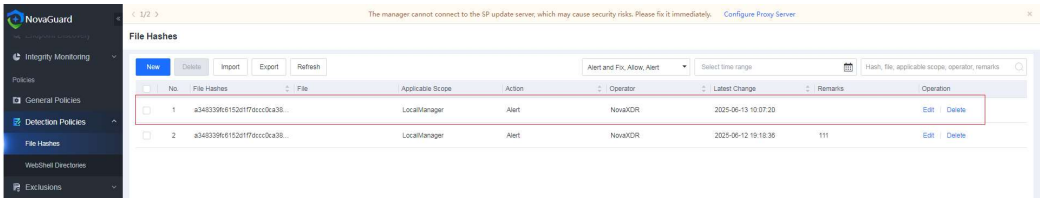
1. After security incidents or alerts are fixed on NovaXDR, the administrator can push malware scan policies from NovaXDR to ensure no malicious files remain on endpoints.





2. MD5 hashes of malicious files can be pushed from NovaXDR to endpoints to quarantine the corresponding files.

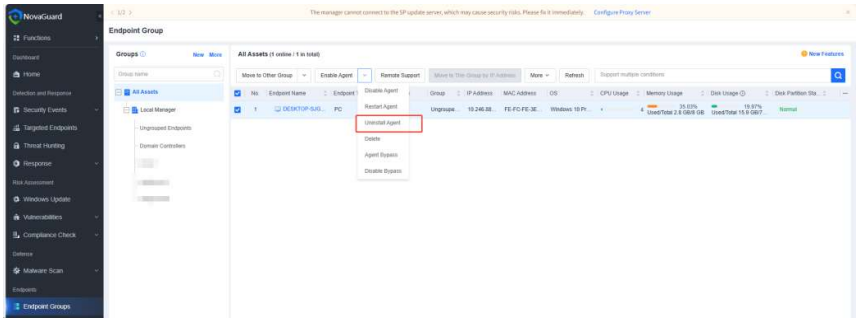




2.5 NovaGuard (SaaS) Feature Improvement

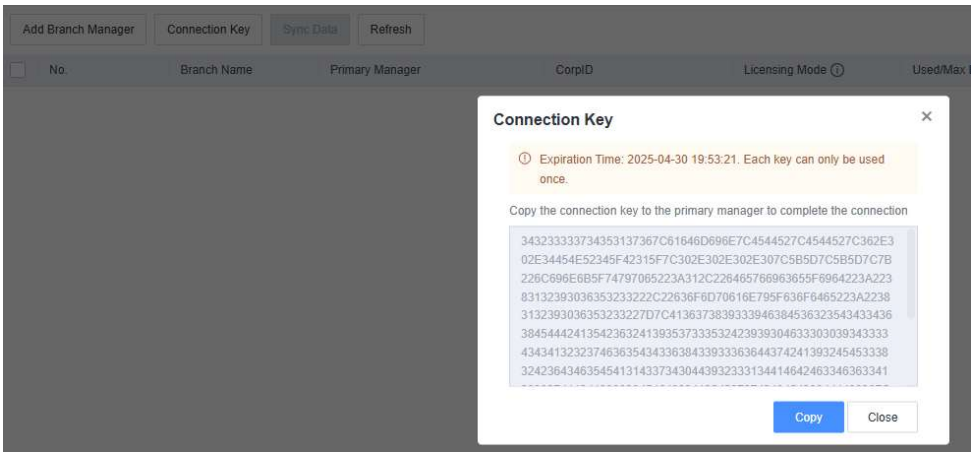
2.5.1 Agent Uninstallation After License Expiration

Within 30 days after the NovaGuard (SaaS) license expires, the administrator can access the console and uninstall the agent.



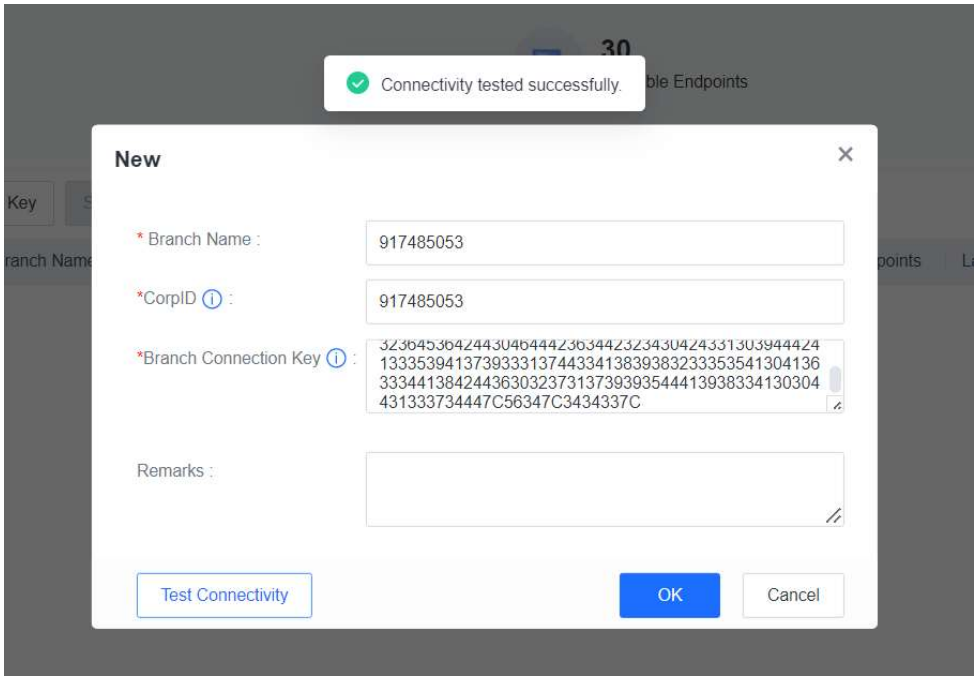
2.5.2 Cascade Deployment of NovaGuard (SaaS)

Step 1. On the branch manager B, create a connection key and copy it.

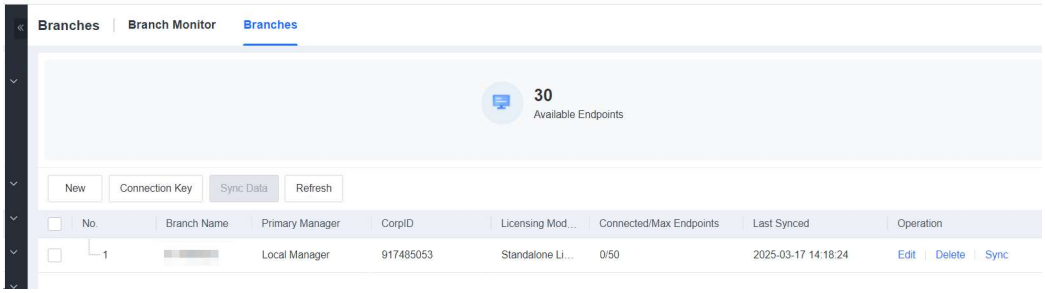


Step 2. On the primary manager A, add a new branch by entering the

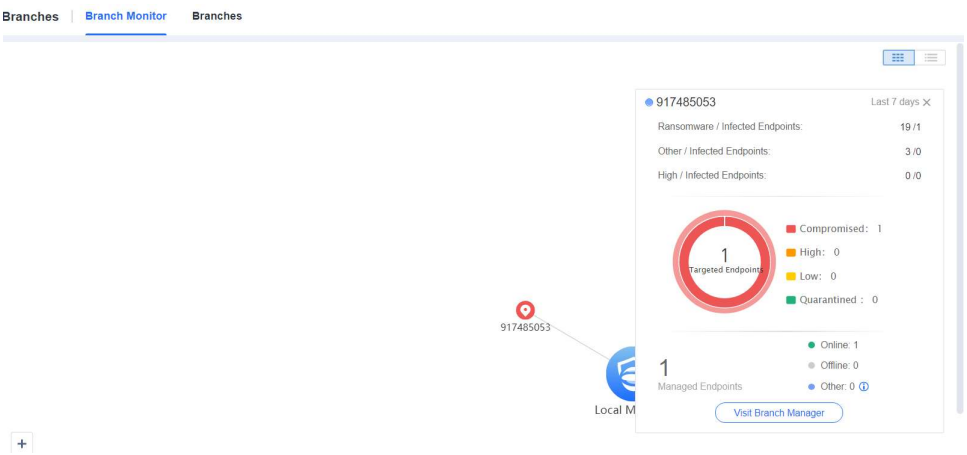
branch name, CorpID, and branch connection key, then save the settings.



Step 3. After the settings are saved, the branch is connected successfully.

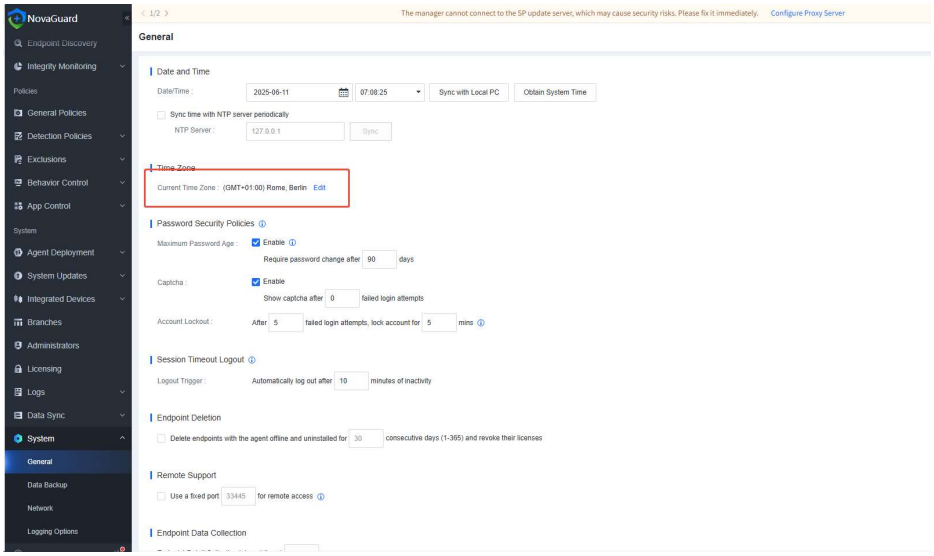


Step 4. Synchronize data of the branch.

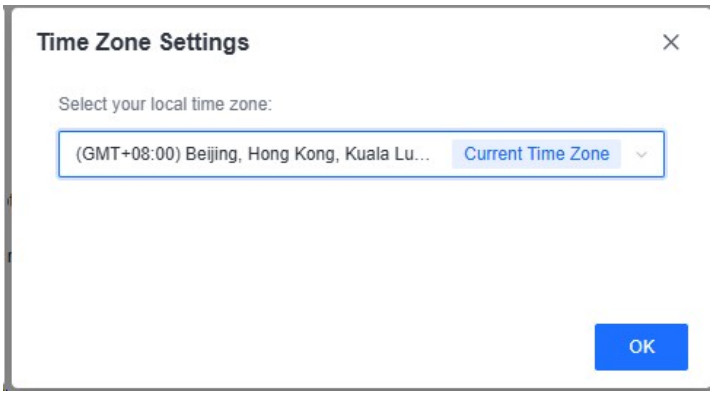


2.5.3 Custom Time Zone Settings

NovaGuard (On-Premises) and NovaGuard (SaaS) support custom time zone settings. A pop-up prompts the current time zone during the initial deployment. The administrator can confirm or modify the time zone.

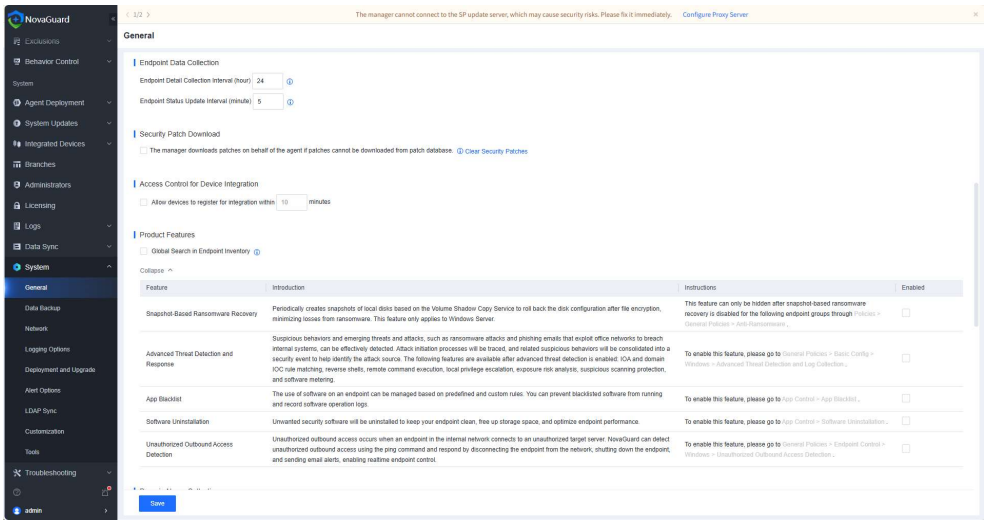


After the deployment is complete, NovaGuard (SaaS) supports manual time zone switching.



2.6 Lag and Stuttering Reduction

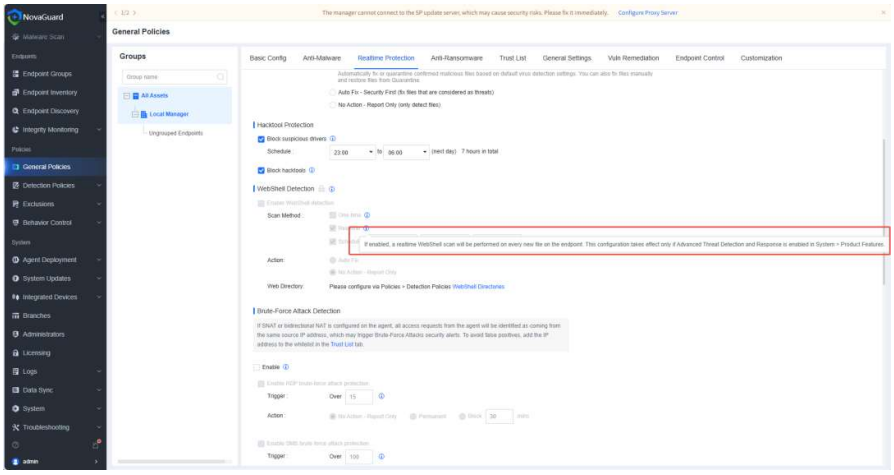
After the upgrade, the following features can be disabled and hidden as needed: Advanced Threat Detection and Response, App Blacklist, Software Uninstallation, Unauthorized Outbound Access Detection, and Cleanup. The administrator can go to **System** > **General** > **Product Features** to enable these features.



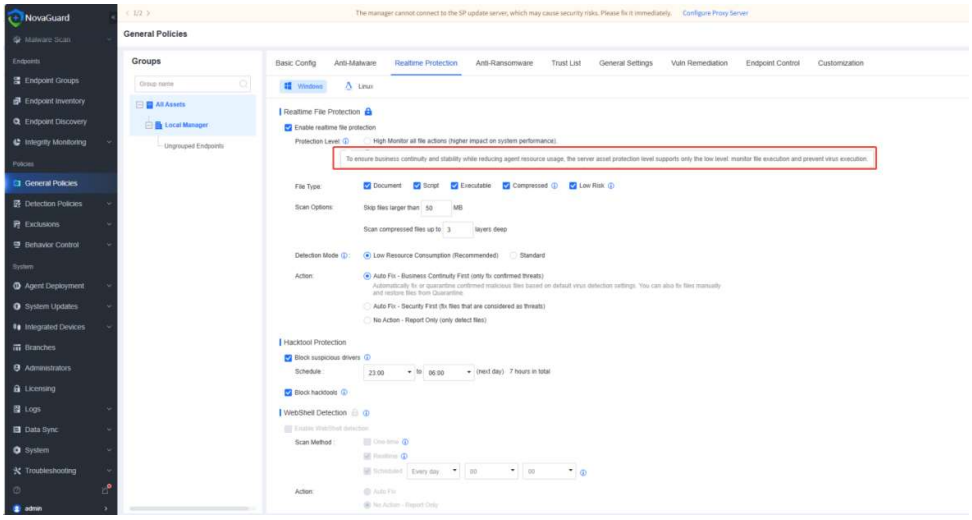
After the upgrade, the **Hot Patching** and **Micro-Segmentation** features will be hidden. To enable these features, please contact technical support.

After the upgrade, the **Enable auto-fix of web intrusions** option will be removed and unavailable.

If the **Advanced Threat Detection and Response** feature is disabled after the upgrade, realtime WebShell detection is not supported for files on Windows and Linux endpoints.

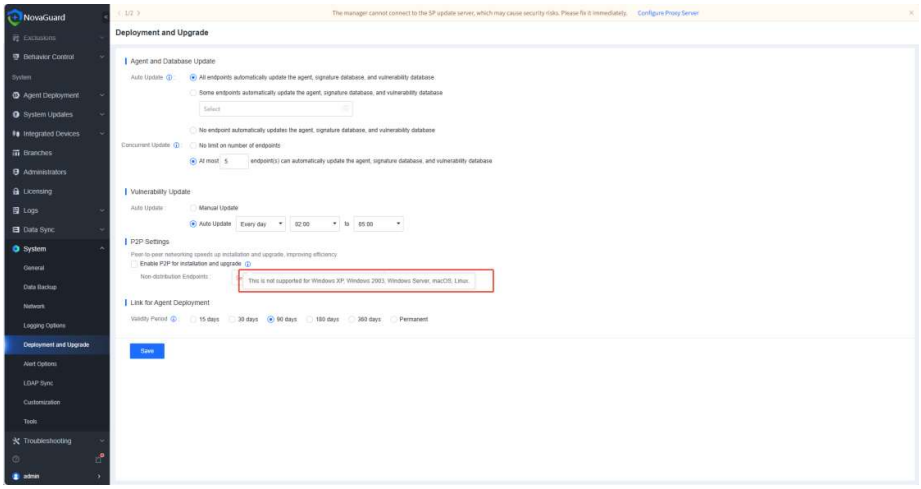


After the upgrade, only low-level realtime file protection is supported for Windows servers. To enable medium- or high-level protection for these endpoints, please contact technical support.

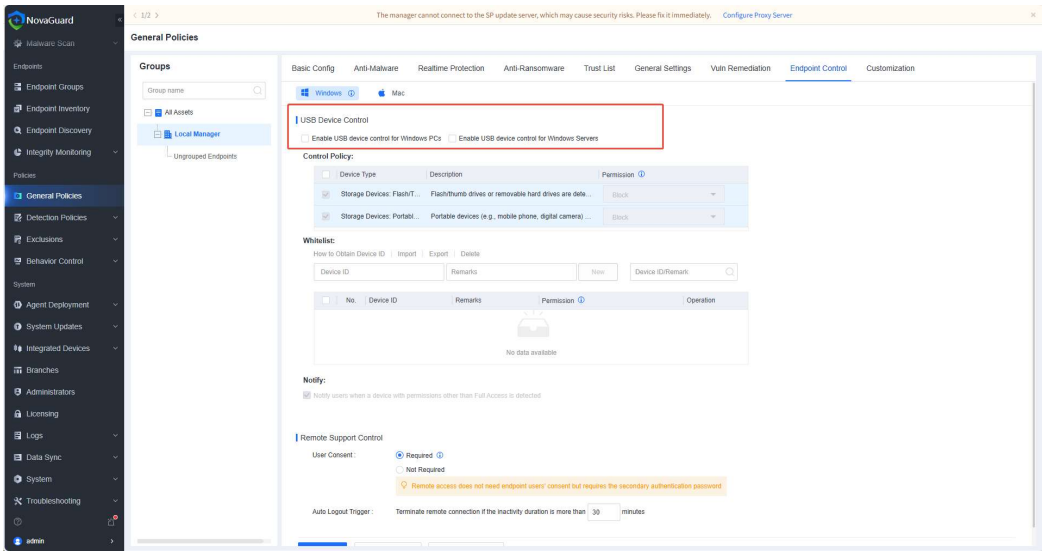


After the upgrade, the memory virus detection feature is not supported for Windows servers. To use this feature, please contact technical support.

After the upgrade, P2P can be enabled for installation and upgrade only on Windows PCs.



After the upgrade, USB device control can be enabled for Windows PCs and Windows servers separately.



2.7 Advanced Threat Detection and Response

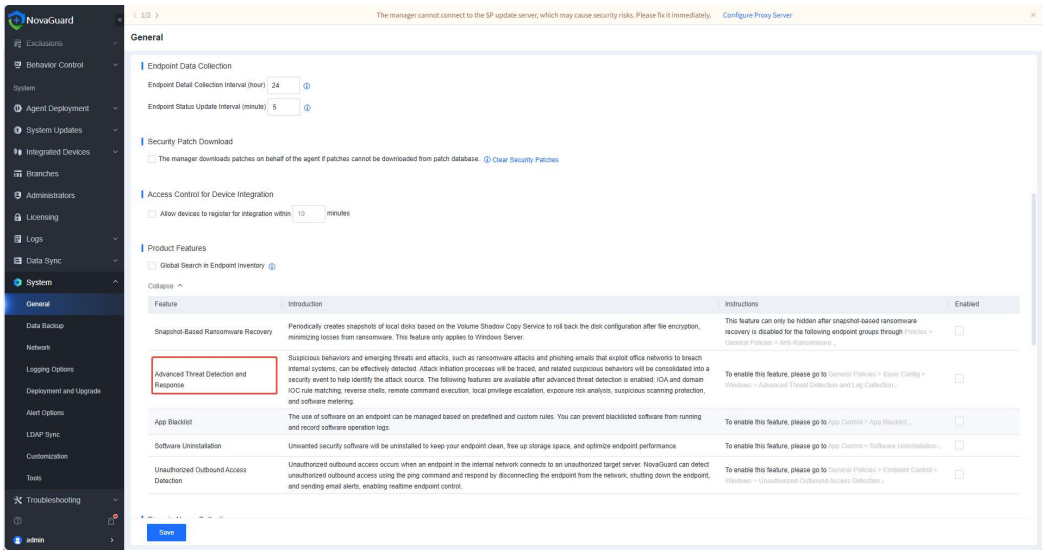
2.7.1 Upgrade Scenarios

1. After NovaGuard Ultimate Edition is upgraded, the **Advanced Threat Detection and Response** feature will be displayed but disabled by default on the **System** > **General** page if no device integration was configured before the upgrade.

2. After NovaGuard Ultimate Edition is upgraded, the **Advanced Threat**

Detection and Response feature will be displayed and enabled by default on the **System** > **General** page if devices were integrated before the upgrade.

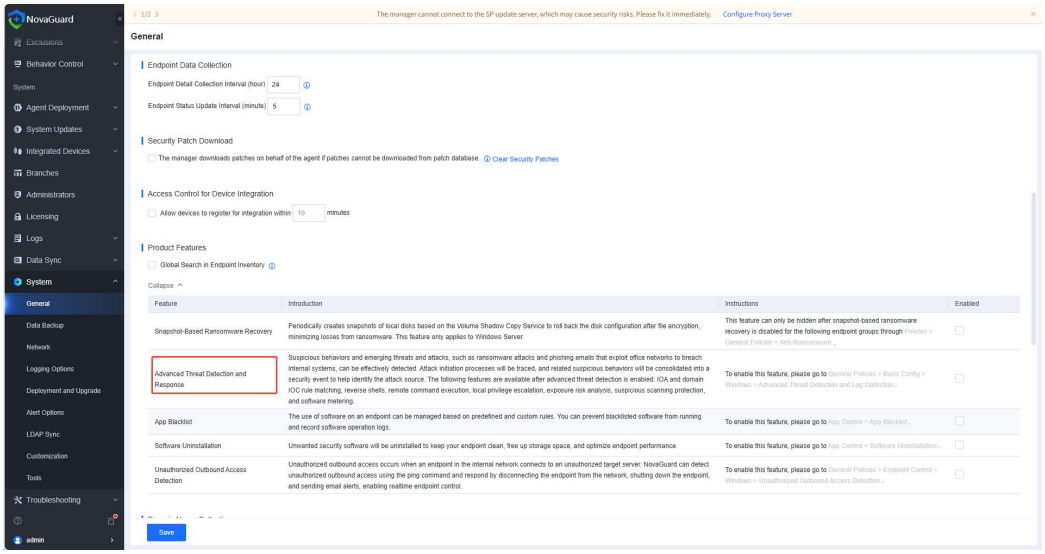
3. After NovaGuard Lite Edition is upgraded, the **Advanced Threat Detection and Response** feature will be displayed and enabled by default on the **System** > **General** page.



2.7.2 Deployment Scenarios

1. After NovaGuard Ultimate Edition is deployed, the **Advanced Threat Detection and Response** feature will be displayed but disabled by default on the **System** > **General** page.

2. After NovaGuard Lite Edition is deployed, the **Advanced Threat Detection and Response** feature will be displayed and enabled by default on the **System** > **General** page.



2.7.3 License Edition Switch Scenarios

1. After NovaGuard Ultimate Edition is deployed, the **Advanced Threat Detection and Response** feature will be displayed but disabled by default on the **System** > **General** page.

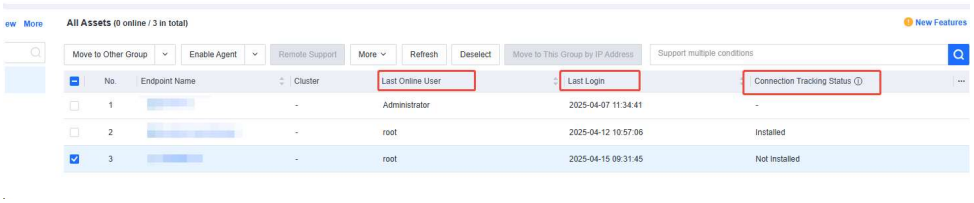
2. After NovaGuard Lite Edition is deployed, the **Advanced Threat Detection and Response** feature will be displayed and enabled by default on the **System** > **General** page.

2.8 Optimized Endpoint Management

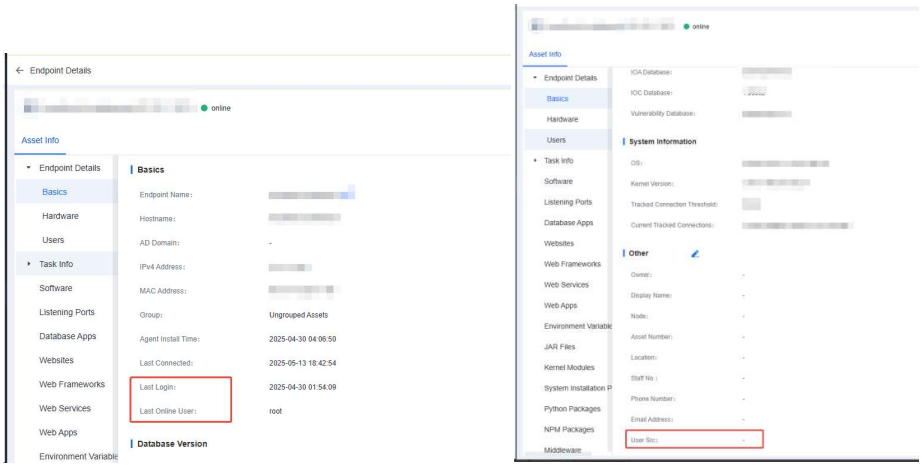
2.8.1 Optimization of Endpoint List and Endpoint Details

1. Added the following fields to the endpoint list on the **Endpoints** > **Endpoint Groups** page: **Display Name**, **Last Online User**, **Last Login**, and **Connection Tracking Status**. Data can be exported from these fields.

   Connection tracking status is supported only for Linux endpoints. For Windows and macOS endpoints, a hyphen (-) is displayed in the **Connection Tracking Status** column, indicating that the feature is not supported.



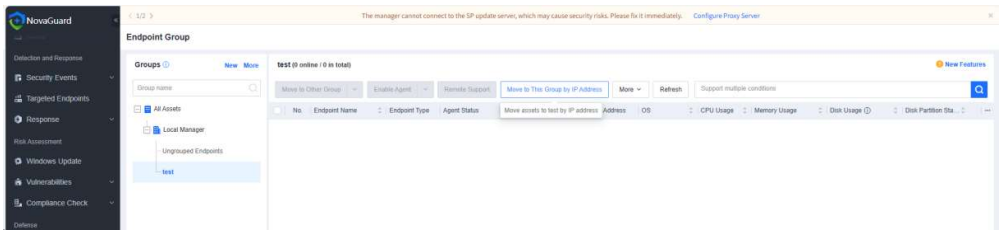
2. Added the following fields to endpoint details: **User Src**, **Last Online User**, and **Last Login**.



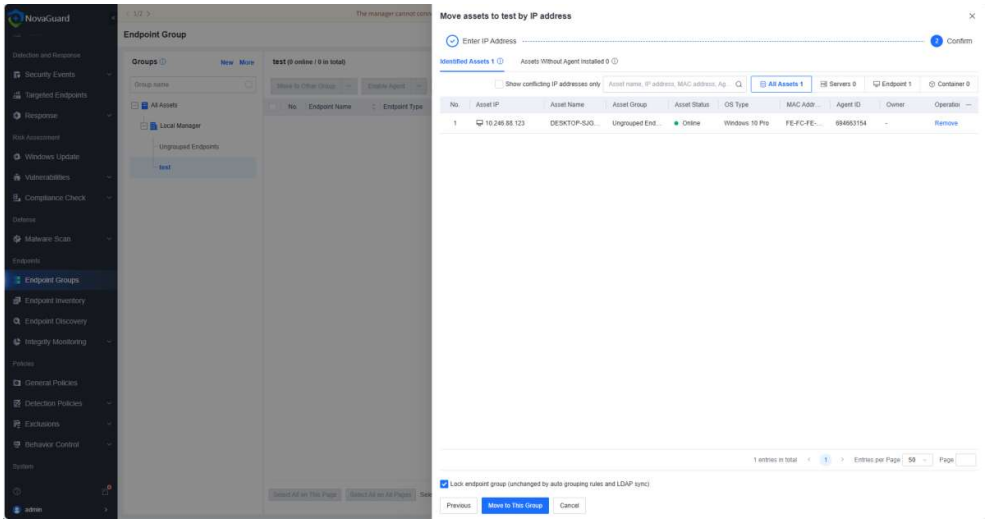
2.8.2 Move to This Group by IP Address (New Feature)

To move endpoints to an endpoint group after exporting the endpoint information from the CMDB system, select the endpoint group and click **Move to This Group by IP Address**.





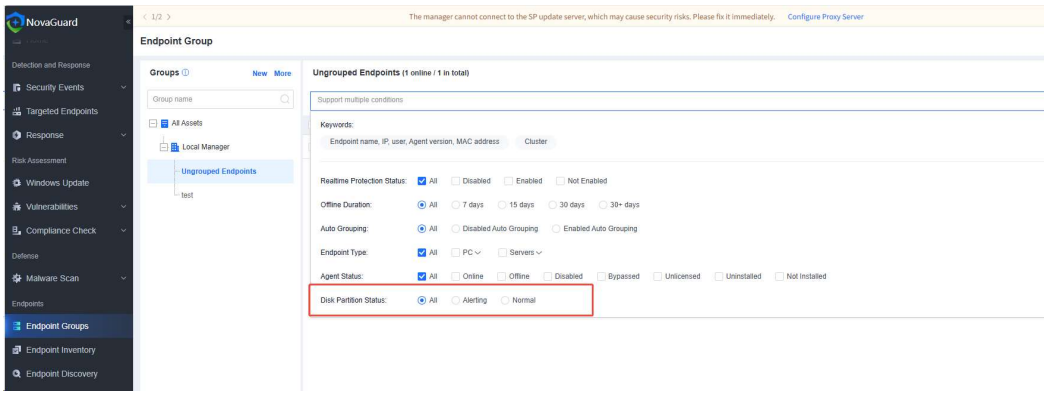
In the panel that appears, enter IP ranges to find the matched endpoints and then click **Move to This Group**.

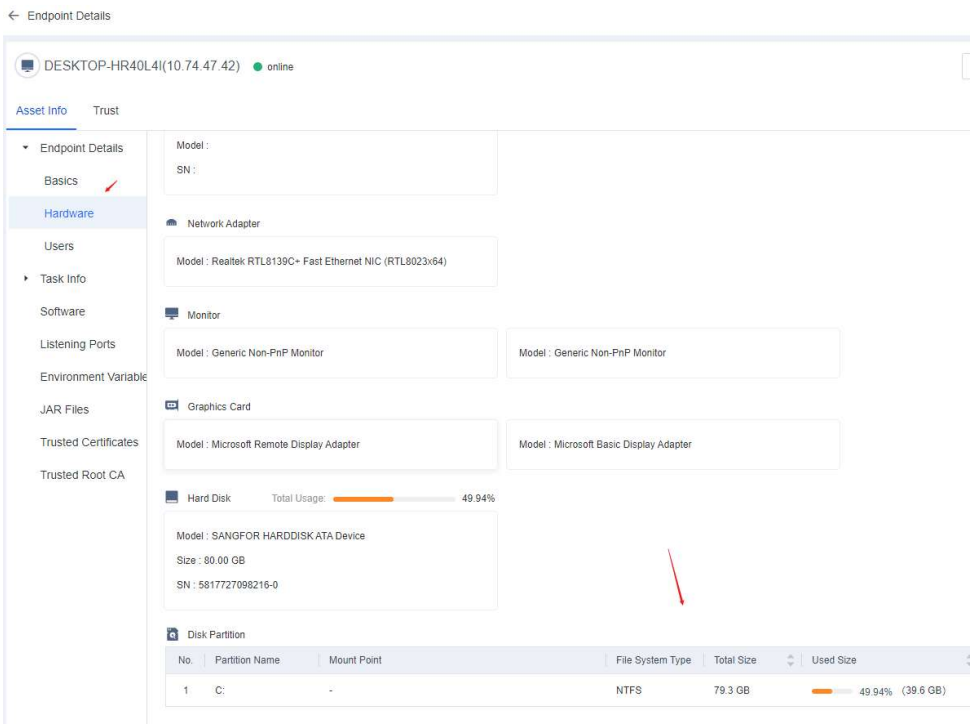


2.8.3 Display of Disk Usage

Supports displaying **Disk Usage** and **Disk Partition Status** to help identify endpoints that exceed the corresponding thresholds.

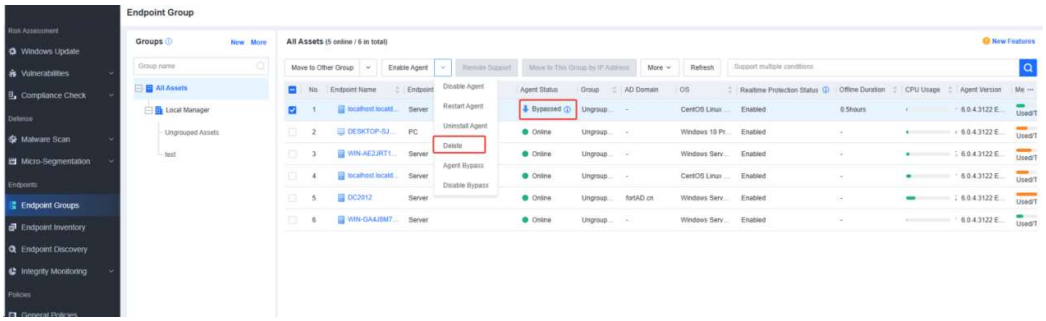


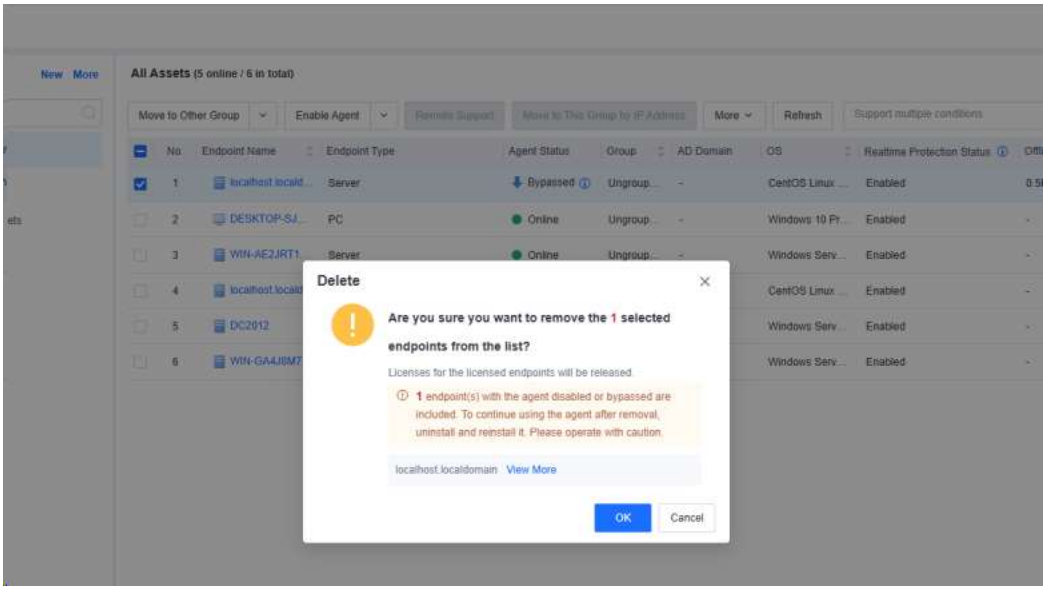




2.8.4 Removing Endpoints with Agent Disabled and Bypassed

The administrator can remove endpoints with the agent disabled and bypassed on the **Endpoints** > **Endpoint Groups** page. (Offline endpoints can also be removed after the upgrade).

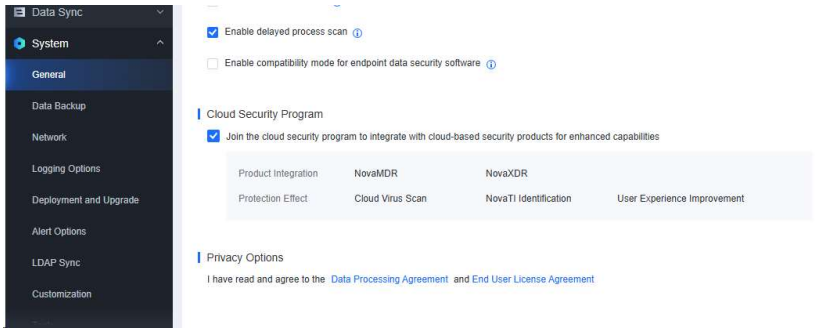




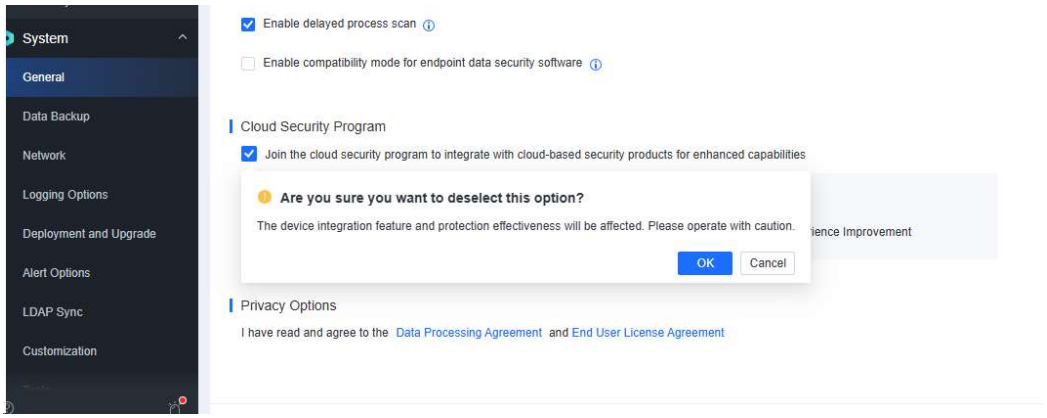
2.9 EULA and DPA Optimization

3. When logging in to NovaGuard for the first time, the administrator needs to enter the username and password, and select **I have read and accept the EULA | DPA**. After the administrator enters the console, DPA will not appear in pop-ups again, and **Join the cloud security program to integrate with cloud-based security products for enhanced capabilities** will be selected by default.

4. The features and protection effectiveness affected by the update of the cloud security program are displayed.

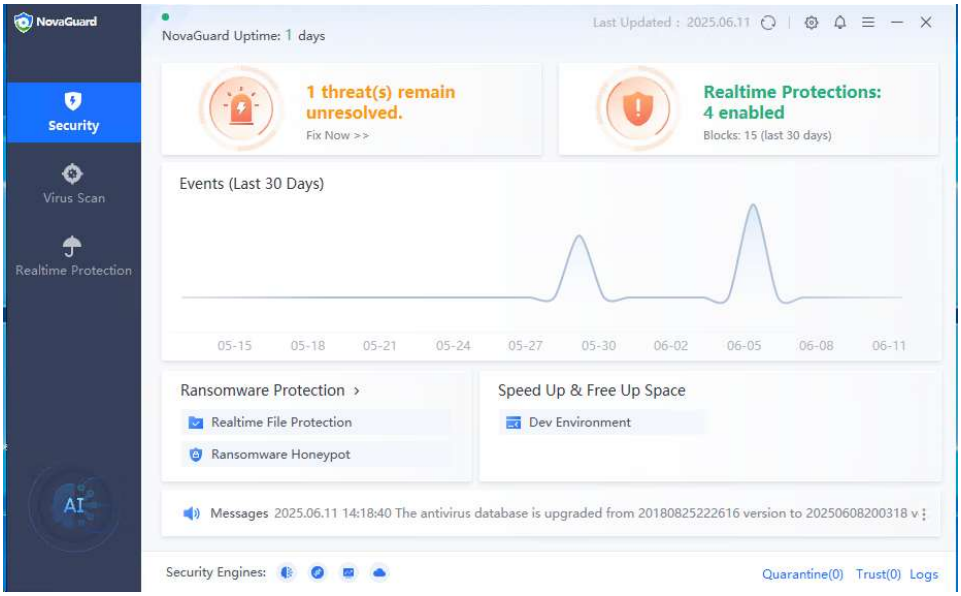


5. A reminder will appear on the page when you deselect **Join the cloud security program to integrate with cloud-based security products for enhanced capabilities**.



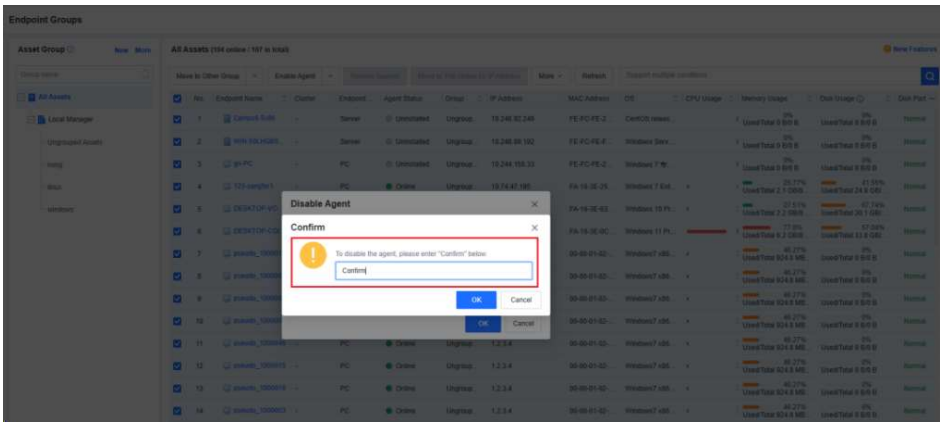
2.10 NovaGuard Agent UI Update

Unified UI style for agent windows.

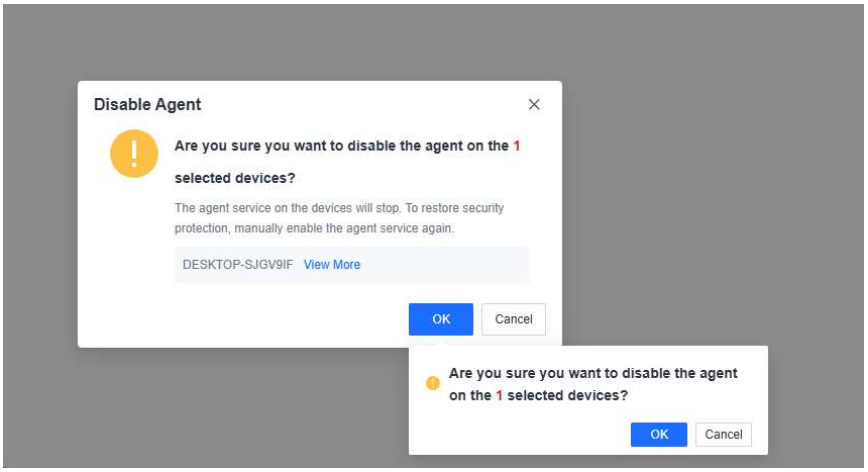


2.11 O&M Operation Optimization

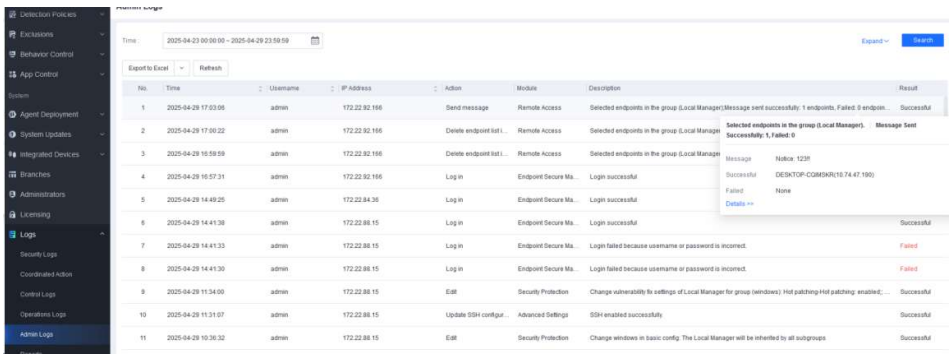
To perform O&M operations (such as disabling, enabling, uninstalling, removing, and bypassing the agent, and disabling agent bypass) and high-risk operations (such as endpoint shutdown, endpoint restart, message notification, and endpoint migration) to 100 or more endpoints, the administrator must enter **Confirm** in the secondary confirmation dialog box.



To perform these O&M and high-risk operations to less than 100 endpoints, the administrator must click **OK** in the dialog box.



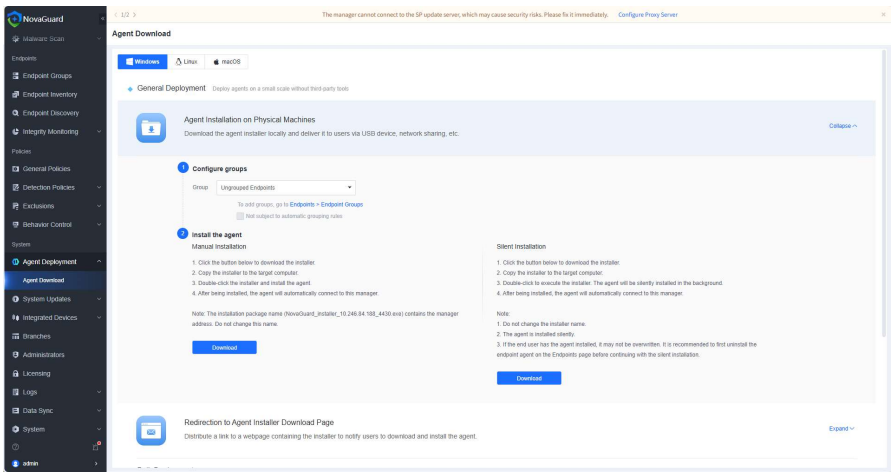
After the O&M or high-risk operations are performed, the administrator can view the results and details on the **System** > **Logs** > **Admin Logs** page.



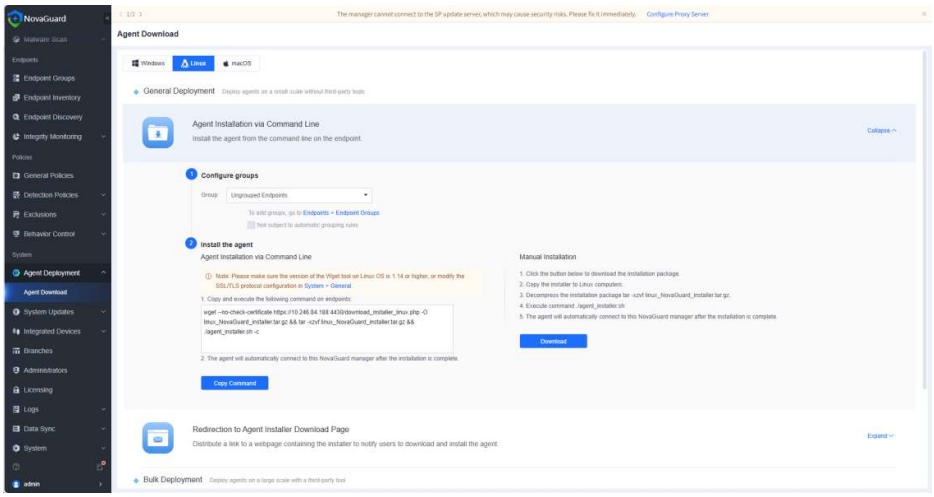
2.12 Installation by Endpoint Group

The administrator can specify a group of endpoints for agent installation. This reduces manual operations and minimizes policy mismatch issues caused by delayed or incorrect manual grouping.

To specify a group of Windows endpoints for agent installation, go to **System** > **Agent Deployment** > **Agent Download**, click the **Windows** tab, select the group, and click **Download**.

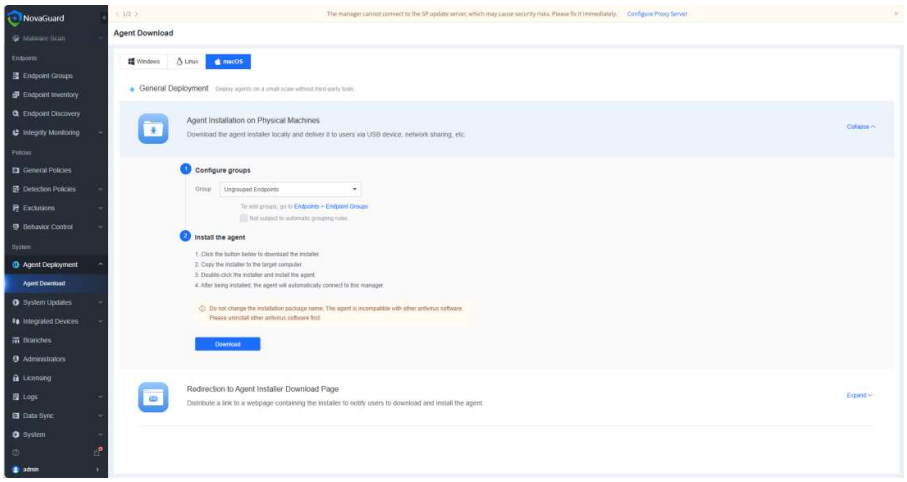


To specify a group of Linux endpoints for agent installation, go to **System** > **Agent Deployment** > **Agent Download**, click the **Linux** tab, select the group, and click **Download**.



To specify a group of macOS Windows endpoints for agent installation, go to **System** > **Agent Deployment** > **Agent Download**, click the **macOS** tab, select

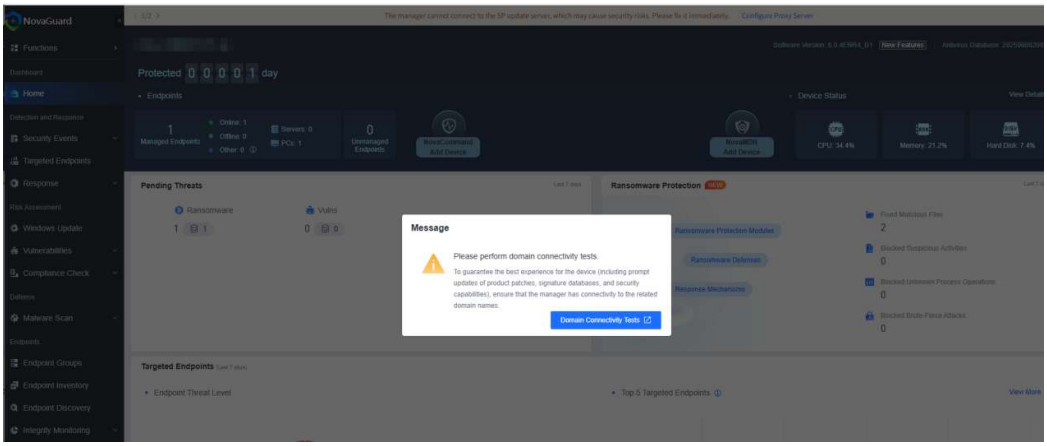
the group, and click **Download**.



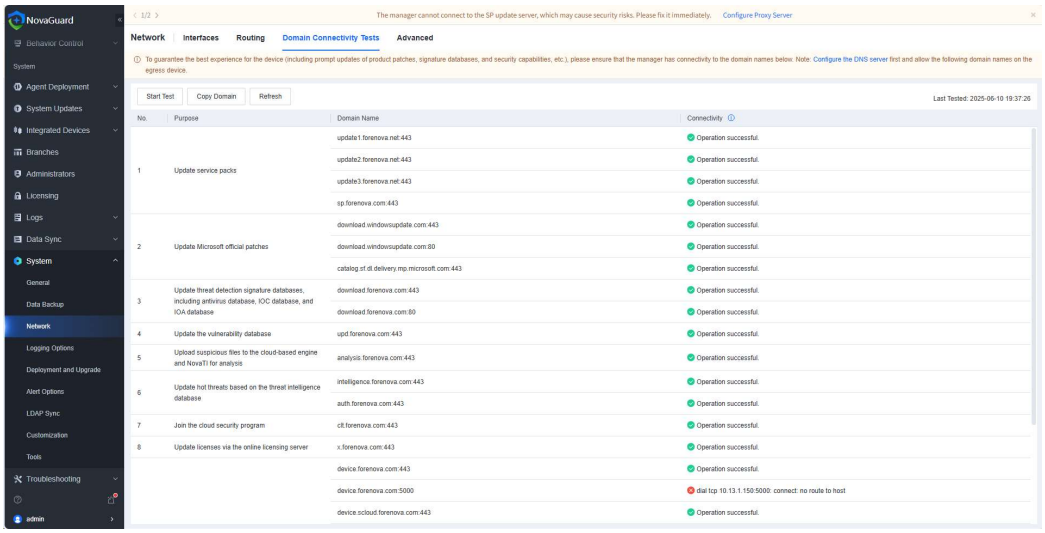
2.13 Domain Connectivity Tests

To guarantee the best experience for the device (including prompt updates of product patches, signature databases, and security capabilities), domain connectivity tests need to be performed after the manager is deployed.

After the administrator logs in to the manager, a pop-up window prompts the administrator to perform domain connectivity tests.



Go to the **System** > **Network** > **Domain Connectivity Tests** page as promoted to start domain connectivity tests.



2.14 Optimization of Other Features

1. Fixed OpenSSH vulnerabilities (CVE-2024-6387 and CVE-2023-28531) in the NovaGuard manager deployed via an ISO or OVA image.
2. Reduced endpoint lag and stuttering, and optimized the realtime protection and antivirus performance of core agent services by increasing process caches and improving the scan logic for low-risk, high-frequency files.
3. Supports automatic recovery of folders and files hidden by worm viruses after virus detection and removal. Updated the malware detection engine to the latest version to enhance detection capabilities.
4. Fixed potential MongoDB database corruption issues during version upgrades or SP installation.
5. Added the Last Online User and Last Login fields to the endpoint list.
6. Supports Tcpdump-based O&M troubleshooting for the NovaGuard manager deployed via an image, improving troubleshooting efficiency.
7. Added the Endpoint IP field to the malware list to improve search efficiency.
8. Retains the entered username and password when the verification code for console login is incorrect or expired.
9. Moved password security policies and session timeout logout settings from the **System** > **Administrators** page to the **System** > **General** page.