# Table of Contents

Endpoint Detection and Response Overview ................................................................. 3  
User Permissions for Endpoint Detection and Response ............................................. 4  
Activate Endpoint Detection and Response ............................................................... 6  
Add an Endpoint Detection Profile ............................................................................ 7  
Install EDR Manually on a Device ............................................................................. 9  
Monitoring Endpoint Detection and Response ........................................................... 11  
Reporting ..................................................................................................................... 12  
Existing Contracted or Trial Standalone EDR ............................................................. 14
Endpoint Detection and Response Overview

Endpoint Detection and Response (EDR) is an integrated threat management software from SentinelOne®. Combining N-able™ N-central® with SentinelOne endpoint protection, EDR enables devices to self-defend and heal themselves by stopping processes, establishing quarantine, fixing forward, and rolling back events to keep devices protected.

EDR monitors multiple processes to recognize attacks as they develop and respond at machine speed. This is different from signature-based detection used by traditional AV solutions, which monitors processes as they execute and not the processes that can spawn from them.

EDR provides forensic data to help you mitigate threats quickly, perform network isolation, and protect against newly discovered threats.

Key new integrated features within N-central include deploying EDR agents, configure profiles, and monitor devices from the dashboard.

Deployment to devices is easy to install on one or multiple devices manually or using rules.

What do you want to do?

1. New N-central EDR Account:
   A. Review Permissions for Using EDR
   B. Activate EDR in N-able N-central
   C. Create an EDR Profile
      › Install EDR
      › Install EDR on a Device
   D. Install EDR Using a Rule
   E. Monitor EDR on a Device

2. Existing Standalone EDR Device Rehoming
   A. Differences Between Standalone and Integrated Versions of EDR
   B. Migrating from Standalone EDR to the Integrated Version of EDR
   C. Taking Ownership of the SentinelOne Installation
   D. Moving Devices Back to Standalone EDR
User Permissions for Endpoint Detection and Response

You can set the permissions for administrator interaction with EDR. Permissions in N-able N-central are a method of controlling access to customers and devices based on the user’s roles. The access is the permission the user has to perform work.

Setting the permissions enables the administrator to install EDR on a device and review the EDR status and reports.

1. Click Administration > User Management > Roles.
2. Select an existing role or select Create Role.
3. In the Administration > MSP N-central area, select an option from the drop-down menu for N-able EDR.
Select **Manage** to enable users to install EDR on devices and view status and reports

Select **Read Only** to enable users to view status and reports

Select **None** to disable the EDR functionality from the user

4. Configure any other permissions and click **Save**.

Assign the role to a user who will perform EDR management activities.

For more information on user permissions and assigning roles, see **What are role-based permissions?**
Activate Endpoint Detection and Response

To use EDR with monitored devices, you need to activate the software in N-able N-central. You can activate EDR for specific Service Organizations, Customers, and Sites.

This activity is only available at the System level.

1. Click **Integrations > Integration Management**.
2. For the **Endpoint Detection & Response** row, click **Activate**.

Once activated, you can create a profile that you use when installing on a single device or install using a rule.

As a quick start, you can select **Manage > Setup profiles** from the Integration Management screen.

You can perform further configuration and maintenance by clicking **Integrations > EDR** and selecting:

- **Dashboard** to see the status of devices and an overview of threats and detections
- **Analyze** to provide monitoring and reporting the forensic details of EDR events
- **Profiles** to add and modify EDR profiles
Add an Endpoint Detection Profile

Create profiles for customers with EDR to deploy the agents. An EDR profile is a standard configuration used on all associated devices. When you install EDR, the configuration within the profile is the baseline settings across a customer’s site. This saves time and ensures consistency when deploying to many devices. This activity is only available at the System level.

1. Click **Integrations > EDR > Profiles.**

2. Click **Add Profile.**

3. Complete the settings in the wizard configuration and associated devices and click **Save** in the screen’s lower right corner.

   › NOTE: These settings must be set up as new even if a Standalone EDR account is active. These settings cannot be migrated from an existing standalone EDR account.
For information on the setting options, see EDR Online Help.

The new profile appears in the profiles list. Use this or another profile when installing on a single device or install using a rule.
Install EDR Manually on a Device

Install EDR on a device to prevent malicious attacks. Before you install EDR on a device, you need to:

- Activate EDR for the Service Organization, Customer, or Site
- Create EDR profiles

For more information on EDR, see Endpoint Detection and Response overview.

1. As an MSP, Click **Views > All Devices**.
2. Click the name of the device you want to edit.

3. Click **Settings > Endpoint Detection & Response**.
4. Click **Enable Endpoint Detection & Response**.

5. Select a profile. You can also choose to create a new profile.

6. Select to install EDR on the device immediately or during a maintenance window.

7. Click **Save**.

N-able N-central installs the EDR software and reboots the device at the next maintenance window.
Monitoring Endpoint Detection and Response

View the status of EDR on a device using several standard facilities within N-able N-central.

ALL DEVICES PAGE

On the All Devices page, you can quickly see which devices have EDR installed. In the Features column, there is some indication. Hover your mouse over the icon to see a quick view of the EDR details on the device.

Services

EDR STATUS SERVICE

The N-able N-central monitoring services provide a summary of the EDR status on a device. The EDR Status service enables you to see the current state of the EDR agent. Monitoring the EDR status allows you to be aware of any issues a technician can resolve quickly and ensure the customer’s endpoint is secure.

1. Click Views > All Devices and click the name of the device.
2. Click Monitoring > Status.
3. Click the EDR Status service.

Click the tabs to adjust the service configuration.

Set up device agent state notifications.
Reporting

Online reports are built-in, customizable reports in N-able N-central to enable you to extract real-time data about the EDR status on devices. Many of the standard reports include information regarding EDR for a device. To access the reports, click the Reports menu.

ADMINISTRATIVE

› License Usage

Services and Processes show SentinelOne.

Integration Management › EDR › Dashboard › Endpoints shows “Pending Request.” Details show reboot pending.
The SentinelOne agent is automatically installed on the device and the user can see the status, if desired.
Existing Contracted or Trial Standalone EDR

DIFFERENCES BETWEEN STANDALONE AND INTEGRATED VERSIONS OF N-ABLE EDR

For a variety of very valid technical, security, and business-related reasons, there are feature differences between the standalone and integrated versions of N-able EDR. Our partners need to understand those differences before they migrate to the integrated version of N-able EDR, so they have a clear set of expectations and workflows.

Notable differences between the two versions include:

- The integrated version does not have the capability to deploy N-able EDR to Linux® devices
- The SentinelOne API is not available for the N-central account.
- The integrated version controls all of the EDR-specific settings via Profiles, whereas those settings are controlled with Groups in the standalone version. This will not impact users that begin with the integrated version.
- To be included in a future N-central EDR release:
  - Notifications: The standalone version allows partners to configure threat notifications to be sent from the EDR cloud console; the integrated version does not allow this option to be configured.
  - Account (MSP)-wide exclusions: The integrated version cannot configure Account (MSP)-wide exclusions.
  - EDR Reports are not available in N-central.
  - Auditing is not available in N-central.

Migrating from Standalone EDR to the Integrated Version of EDR

Migrating from the standalone version of N-able EDR to the integrated version is a straightforward process that only requires a few steps:

- Follow the steps described to Activate EDR in N-central found in the New N-central EDR Account
- We suggest migrating a subset of devices and test and understand the N-central EDR feature set.
**Taking Ownership of the SentinelOne Installation**

Devices will not bring existing threat information when rehomed. These devices will act as newly installed devices.

If the device is managed by N-central already and has EDR installed on it, one of two things will happen:

- Suppose that EDR install is reporting into a standalone EDR account owned by N-able. In that case, we will take ownership of that EDR install and will rehome the device from the standalone EDR cloud account to the integrated EDR cloud account.
- If that EDR install is reporting into a standalone EDR account not owned by N-able, the install migration process will not be successful. This is because we (N-able) don’t have access to the SentinelOne cloud account’s uninstall password. In this situation, the partner will need to remove the currently installed EDR agent from their standalone EDR cloud console.

**Moving Devices Back to Standalone EDR**

To move a device from N-central with EDR back to Standalone EDR:

- Uninstall EDR agent from N-central device.
- From the SentinelOne Dashboard, download and install the standalone SentinelOne agent package.