

Nextthink V6.1

User Manual

Generated: 3/01/2020 6:35 pm

Table of Contents

Getting started	1
Logging in to the Finder.....	1
Logging in to the Portal.....	5
Querying the system	6
Searching the subject of interest.....	6
Executing an investigation.....	8
Creating an investigation.....	9
Editing the options of an investigation.....	11
Navigating through the results of an investigation.....	17
Comparing the properties of users and devices.....	22
Visualizing system activity in the Finder	25
Getting a quick overview.....	25
Graphically observing the activity of users and devices.....	26
Observing service performance.....	35
Viewing network connections.....	40
Viewing web requests.....	44
Viewing executions.....	47
Monitoring IT custom metrics	52
Creating a metric.....	52
Examples of metrics.....	58
Following the evolution of a metric.....	61
Monitoring IT services	65
Analyzing service quality.....	65
Creating a service.....	67
Following the evolution of a service.....	71
Specifying URL paths of web-based services.....	72
Organizing objects with categories	74
Classifying objects of the same type.....	74
Creating categories and keywords.....	75
Tagging objects manually.....	77
Tagging objects automatically.....	78
Importing tags from text files.....	80
Nextthink Application Library.....	82

Table of Contents

Getting notified by the system.....	85
Receiving alerts.....	85
Creating a service-based alert.....	89
Creating an investigation-based alert.....	91
Building web-based dashboards.....	95
Introducing dashboards in the Portal.....	95
Creating a dashboard.....	96
Examining metrics in depth.....	97
Assessing license use.....	98
Computing dashboard data.....	104
Reusing dashboard content.....	113
Importing and Exporting authored content.....	116
Methods for reusing authored content.....	116
Manually sharing Finder content.....	117
Importing a content pack.....	119
Conflict resolution.....	120
Exporting a content pack.....	124

Getting started

Logging in to the Finder

To start working with the Finder, authenticate first as a valid user. Sign in with your dedicated Nextthink account credentials or, alternatively, use your Windows credentials if your administrator has enabled the authentication through Active Directory.

The login process starts by connecting the Finder to the Portal. From the Portal, the Finder retrieves first the list of available Engines within your view domain and finally connects to the Engine of your choice. Once connected, the Finder has access to the data stored both in the Engine and in the centralized content manager of the Portal; letting you visualize, organize, and query end-user data in a variety of ways.

Quick connect

When you run the Finder for the first time, the login dialog appears in *Quick connect* mode, as indicated by its title at the top left corner of the dialog. Quick connect mode lets you specify all the necessary credentials to connect to any Portal. To log in to the Finder in Quick connect mode:

1. Fill in the **Host : Port** field with the DNS name or IP address of the Portal to which you want to connect, optionally followed by a colon and the port number where the Portal is listening for connections (by default, 443).
2. Type in your **Username**, which is the name of the user as registered in the Portal.
3. Type in your **Password**.
4. Optional: Check the option **Remember me** to have the **Host : Port** and **Username** fields prefilled with the same data that you just typed the next time that you log in to the Finder from the same computer. You have to retype your password only.
5. Optional: Check the option **Sign me in automatically** for the login dialog to remember your password as well and skip the login step altogether the next time that you run the Finder from the same computer. Checking this option implies that the previous **Remember me** option is also checked.
6. Click **Connect**.
7. If more than one Engine within your view domain is available in the Portal, a list with all connected Engines shows up in the dialog **Engine selection**:
 - ◆ Click the name of an Engine to connect to it.

- ◆ Click the star to the right of the name of an Engine to make that Engine your favorite. The next time that you log in to the Finder from the same computer, the step to select the Engine is skipped and you connect directly to your favorite Engine. You can later change your favorite Engine once you have logged in.

If the Finder cannot connect to the Portal or to the selected Engine, it aborts the login process and displays an error message with the reason for the failure. For warnings related to security certificates during the connection, see the section on certificate issues below.

Creating a session

In a multi-user or multi-Appliance environment (e.g. an environment with test and production Appliances), you may have to log in to the Finder with distinct user accounts and connect to different Appliances from a single post. In these cases, to save you from typing the credentials every time that you have to log in to a different Appliance, store the credentials for distinct users and associated Appliances into *sessions*. Later, log in to the Finder faster by accessing your stored sessions.

To create a new session in the login dialog:

1. Click the **+New** button found at the top right corner of the login dialog. The login dialog turns into *session creation mode*, copying the information that you typed previously in Quick connect mode, if any, or from a previously selected session into the fields **Host : Port** and **Username** of the new session. Note that sessions do not store passwords by default. You can later specify to remember your password if you frequently use the same session.
2. Type in the DNS name or IP address of the Portal appliance, followed by a colon and the port number where the Portal is listening for connections in the field **Host : Port**. You can keep the copied value, if any.
3. Type in the name of the user to store in the session in the field **Username**. Again, you can keep the copied value, if the name of the user is not empty.
4. Optional: Change the name of the session that is displayed at the top of the dialog by clicking on it and typing an alternative name. By default, the name of the session is built from the name of the user and the Portal appliance in the form: *Username on Host : Port*.
5. Click **Create** to save the session. The login dialog switches now to *session mode*.

Note that sessions are created locally in your instance of the Finder. Therefore, the sessions that you create in one computer are not automatically available when you try to log in to the Finder from another computer.

Using a session to log in

Once you have created one or more sessions, you can use them to quickly log in to different Engines. You only have to select the appropriate session and, eventually, enter your password. To log in from a saved session from the login dialog:

1. Click the down arrow in the top left tab of the login dialog, to the right of its title. A drop down list appears with the names of the saved sessions and the **Quick connect** option at the top.
2. Select one of the saved sessions. The user and Engine information stored in the session are displayed in the dialog. If you select **Quick connect** instead, you go back to Quick connect mode. Read the previous section on using the login dialog in Quick connect mode.
3. Type in your password.
4. Optional: To store your password with the session information, check the option **Remember password**.
5. Optional: Check the option **Sign me automatically** to skip the login step altogether and start the connection to the Engine of the selected session as soon as you open the Finder. This option requires the **Remember password** option to be checked.
6. Click **Connect** or press **Enter** and the Finder starts to establish a connection to the chosen Portal.
7. If more than one Engine within your view domain is available in the Portal, a list with all connected Engines shows up in the dialog **Engine selection**:
 - ◆ Click the name of an Engine to connect to it.
 - ◆ Click the star to the right of the name of an Engine to make that Engine your favorite. The next time that you log in to the Finder from the same computer, the step to select the Engine is skipped and you connect directly to your favorite Engine. You can later change your favorite Engine once you have logged in.

If the Finder cannot connect to the Portal or to the selected Engine, it aborts the login process and displays an error message with the reason for the failure. For warnings related to security certificates during the connection, see the section on certificate issues below.

Editing a session

If one of your saved sessions has wrong data or there was a change in user or Appliance settings, you may want to edit the session. To edit the values stored in a session:

1. Click the down arrow placed in the top left tab of the login dialog (to the right of the title) and select the session that you want to edit from the drop down list.
2. Click the **Edit** button that you find at the top right corner of the login dialog. You enter session edition mode.
3. Edit the fields **Username**, **Host : Port** and the name of the session in the same way as you did when creating the session (see previous section).
4. Click **Save** to save your changes and go back to session mode.

Deleting a session

When you do not need a session anymore, remove it from your list of sessions. To delete a session from the login dialog:

1. Click the down arrow placed in the top left tab of the login dialog (to the right of the title) and select the session that you want to delete from the drop down list.
2. Click the **Delete** button that you find at the top right corner of the login dialog. A dialog appears asking you for confirmation on deleting the session.
3. Click **Yes** to confirm that you really want to delete the session. The login dialog removes the session from the list and goes back to Quick connect mode.

Certificate issues

While connecting to the Portal or to the Engine of your choice, the Finder may display a warning message about security certificates on a dialog with the title:

There is a problem with the Portal / Engine security certificate

Security certificates ensure that the connections among Nextthink components are safe. A problem with the certificates implies that there is a potential risk of impersonation. In particular, if you use the default self-signed certificates from Nextthink (or any other certificate not signed by a trusted CA), you can read the following message in the dialog:

The security certificate of Nextthink Portal / Engine could not be validated.

If you are testing the solution or you are sure that the certificate is correct:

1. Optional: Click **Show certificate** to display detailed information about the current certificate.
2. Optional: Tick the option **Do not notify me again for this certificate** if you want to accept the current certificate as valid and avoid the warning in subsequent logons.
3. Click **Continue anyway** to go on with the login process despite the warning message.

Otherwise, contact your administrator for replacing the certificates. Log in only after your administrator has finished installing the new security certificates.

Related tasks

- Adding users
- Preventing password saving in the Finder
- Importing and replacing Certificates
- Active Directory authentication

Logging in to the Portal

Sign in to the Portal with your dedicated Nextthink account credentials or, alternatively, use your Windows credentials if your administrator has enabled the authentication through Active Directory.

To log in to the Portal:

1. Open your favorite web browser (check the list of supported web browsers in the release notes of the Portal).
2. Type in the name or IP address of the Portal in the address bar of the browser.
3. On the login dialog, type in your credentials:
 1. Type in your user name under **Username**.
 2. Type in your **Password**.
4. Optional: Tick the box **Remember me** for the Portal to automatically fill in the Username field the next time that you log in.
5. Click **Sign in**.

Querying the system

Searching the subject of interest

Searching in the Finder

The Finder offers you many different possibilities to get information about your IT infrastructure. To help you find your way through, the Search box in the Start page is the best place to get started with the Finder. The Search box is a valuable tool for both beginners and experienced users and it can save you lots of time by directly bringing useful information to your fingertips. To look for a particular piece of information in the Finder, just type what you are looking for in the Search box.

To search in the Finder with the Search box:

1. Locate the Search Box at the top of the Start page, placed to the right of the Nexthink logo and labelled with the legend *What are you looking for?*. The Search box has a distinctive magnifying glass on its right side.
2. Type related terms to the subject of interest in the Search box. The magnifying glass in the box turns into a circular progress indicator followed by a cross. Results show up in the Start page as you type.
3. Optional: Click the cross to cancel the current search and erase both the Search box and the list of results.

The results of a search are all items and investigations that are related in some way to the words that you typed in. For instance, you can look for users, devices or applications by typing in the first letters of their names. In this way, if you type **nexthink** in the Search box, you get a list with the applications from this company that are installed in your system, such as the Finder and the Collector, along with their executables and binaries, the packages that installed those applications, the devices where they were installed or even the visited web domains that are related to Nexthink, such as `doc.nexthink.com`. Similarly, you can look for investigations related to generic objects by typing the name of the object. For example, if you type in the keyword *printers* in the search box, you get investigations related to printers under the section **Investigations**. You can also search by platform. For example, type `Mac OS applications` to search for applications on the Mac OS platform.

Search results

As an example, let us examine the search results when looking for user *gdaniel*

in the Finder:

The results are divided into two sections:

- The section **Investigations** on the left-hand side of the window.
- The related items section on the right-hand side of the window, which includes the objects, services, metrics, and categories that match the search terms.

The **Investigations** section usually shows both suggested and existing investigations:

- *Existing* investigations are those that have been previously created in the Finder and are available to the current Finder user.
- *Suggested* investigations are those inferred from the search terms and proposed by the Finder on the fly. All suggested investigations in the list are marked with the keyword **Suggested**.

In this specific example, only suggested investigations show up, as there are no existing investigations that include the term *gdaniel*. Each investigation is preceded by an icon that indicates the object on which the investigation is based. Click an investigation on the list to run it.

Result items on the right-hand side of the window are grouped by type. Click the result item to drill-down to it or right-click the item to trigger different actions.

[Click here for more information on how to effectively search in the Finder.](#)

Searching devices in the Portal

The Portal includes a search tool, called *Device locator*, that looks for devices across all connected Engines. To know which Engine receives information from a particular device, enter the name of the device or the name of a user of the device in the Device locator.

To look for a particular device in the Device locator:

1. Click the magnifying glass in the top right corner of the Portal. The Portal brings up the **Device locator**.
2. Type the name of the device or the name of a user that has interacted with the device in the search box labelled *Enter a device or user name*. Incomplete names are allowed.
3. Click **Search** or press **Enter**.
4. Results show up below up to a maximum of ten entries. If necessary, refine your search to reduce the number of matching results. Each entry displays the name of the device, the user that last logged in to the device, the Engine to which the device sends information, and the last time that the device has been seen in the network.
5. Optional: Click the name of the device in the list of results to open the device view of that device in the Finder.
6. Optional: Click the name of the last logged in user in the list of results to open the user view of that user in the Finder.

Related references

- Search in Finder

Related concepts

- Object
- Investigation
- Service
- Category

Executing an investigation

The basic unit to query the Nextthink database is the *investigation*. To execute an investigation in the Finder:

1. Find the investigation that you want to execute by either:
 - ◆ Browsing the **Investigations** section on the left-hand side panel of the main window.
 - ◆ Searching a term in the Search box and looking under the **Investigations** or the **Suggested investigations** sections in the results of the search.
2. Double-click the name of the investigation.
3. The results of the investigation are displayed as a table on a new tab in the Finder.

Related tasks

- Navigating through the results of an investigation
- Searching the subject of interest
- Creating an investigation

Related concepts

- Investigation

Creating an investigation

Investigations let you query the real-time database and look for specific information about objects, activities or events.

To create a new investigation in the Finder, you have different choices:

- [Create an anonymous investigation](#) that you can quickly run. Optionally, you can save the investigation later.
- [Create a named investigation](#) and save it at the time of creation for later reuse.
- [Duplicate an existing investigation](#) that is similar to the investigation that you want to create.
- [Save or edit a drill-down or a one-click investigation](#) from its list of results.

Creating an anonymous investigation

To create an anonymous investigation in the Finder:

1. Click the **New Investigation** button at the bottom of the start page.
2. Edit the options of the investigation.

3. Click the **Run** button to execute the investigation that you just created.
4. Optional: if you want to save the investigation, press **Ctrl+S** or click the floppy disk icon at the top right corner of the window that displays the list of results.

Creating a named investigation

To create a named investigation in the Finder:

1. Go to the **Investigations** section on the left-hand side of the main window.
 - ◆ If you want to place the investigation at the top level of the investigations tree, right-click the header or the empty area of the sub-section **My investigations**.
 - ◆ If you want to place the new investigation inside a particular folder, right-click one of the folders of the sub-section **My investigations**.
2. Select **Create new investigation** from the context menu.
3. A new investigation with the temporary name **Untitled investigation n**, where *n* is a growing number to avoid name collisions, shows up in a new tab. Optional: Click the name of the investigation and replace it with an appropriate name.
4. Optional: Click the field below the name of the investigation labeled **Enter description here...** and give a short description of the purpose of the investigation.
5. Edit the options of the investigation.
6. Click **Save & Run** to save the new investigation and execute it right after.

Duplicating an existing investigation

Creating an investigation from scratch can be a lengthy process because of the many options and settings available for editing the investigation. If you already have at your disposal an investigation that is similar to the investigation that you want to create, you can save a lot of time by duplicating the existing investigation and adapting it to your needs, instead of going through the whole process of creating a new investigation.

To duplicate an existing investigation:

1. Find the investigation to duplicate in the **Investigations** section of the accordion.
2. Right-click the investigation name and select **Duplicate** from the context menu. A new investigation with the name **Copy of A**, where *A* is the name of the existing investigation, is created. A new tab opens the investigation

- for editing.
3. Optional: Click the name of the investigation and change it to something more meaningful than **Copy of A**.
 4. Optional: Change the description of the investigation to reflect the purpose of the new investigation.
 5. Modify the investigation options. Because you selected a similar investigation, there should be only a few options to change.
 6. Click on **Save & Run** to save the investigation and execute it right away.

Saving after navigation

When you navigate through results by drilling-down or executing a one-click, you are effectively executing a new investigation that the Finder creates on the fly. The investigation is discarded as soon as you close the tab that displays the list of results of the drill-down or one-click. However, if you think that the investigation is useful and that you might need it later, you can save it before closing the list of results.

To save an investigation generated by a drill-down or a one-click from its list of results, either:

- Click the floppy disk (save) icon in the top right corner of the window and give a name to the investigation.
- Click the pencil and paper (edit) icon placed to the right of the save icon. You are asked to save the investigation with a name. Additionally, you can edit the investigation settings.

Related tasks

- Editing the options of an investigation

Editing the options of an investigation

To edit the options of an existing investigation, either:

- Right-click the investigation name in the **Investigations** section of the left and select **Edit**.
- Execute the investigation and click the pencil and paper icon that appears in the top right corner of the list of results.

When you create a new investigation or edit an existing investigation, the Finder opens a dialog that lets you set all the options of the investigation.

The first thing that you find at the top of the dialog is the name of the investigation and an optional description of what it does. Click the name or the description to modify their contents.

Below the name and the description, you find three distinct sections that let you design the investigation to get the desired results:

- **Retrieve**
- **Matching**
- **Display**

Retrieve section

In the **Retrieve** section, choose the object, activity or event of interest. The execution of the investigation returns a list of results with items of the selected type.

Platform selection

In the upper-right part of the **Retrieve** section, find three check boxes to select the platforms that are applicable to the investigation. The conditions and display fields that you are able to edit in the investigation depend on the platforms that you select here.

- If you choose one platform, you can use conditions and display fields available for that platform.
- If you select multiple platforms, only those conditions and display fields shared by all the selected platforms are available.

For instance, if you select to retrieve devices of the Mobile platform, you can only set conditions on devices or user fields, because all other objects are not available for Mobile.

In a similar way, if you choose to retrieve an object type that is not available in all platforms, the check boxes of the platforms in which the object is not available are ineligible.

For example, if you choose to retrieve domains, which are only available for the Windows platform, the check boxes of both Mac OS and Mobile platforms are

disabled.

By default, when you create a new investigation, only the Windows platform is ticked in this section.

Matching section

In the **Matching** section, you select the criteria that the objects, activities or events of the type that you chose in the **Retrieve** section must fulfill to appear in the list of results. The **Matching** section is divided into two subsections: **Conditions** and **Time Frame**.

Conditions

The matching **Conditions** are a set of rules that apply to any type of item related to the one selected in the **Retrieve** section. You can set constraints on the properties or categories of objects, activities or events to filter the results of your investigation.

To add a new condition:

1. In the **Conditions** subsection, click the link **Click here to add a new condition**. The placeholders for the condition fields show up.
2. Set the object, activity or event to which the condition applies.
3. Set the attribute or category that you want to constraint.
4. Set the operator for comparison (e.g. *is*, *is not*, *starts with*, etc).
5. Set the matching value, if you selected an attribute constraint, or the matching keyword, if you selected a category constraint.

Some combinations of conditions and display settings are incompatible. If you add a condition and a red exclamation mark appears on its right side, the condition may conflict with another condition or with one of the chosen attributes to display. Hovering the mouse over the exclamation icon will tell you the reason for the conflict. Investigations with conflicting conditions cannot be saved. Deselect the conflicting display attributes or delete the conflicting condition before saving the investigation.

To delete a condition:

1. Click the trash icon to the right of the condition fields.

To make a template investigation:

1. Instead of providing a matching value in the last condition field, click the question mark to its right to transform the investigation into a template investigation. The actual matching value is provided as a parameter when executing the investigation.

By default, the results of an investigation must fulfill all the expressed conditions. That is, the resulting filter is a logical AND of all the conditions. If you want to combine the conditions in a different way:

1. Click the **Advanced** area to expand it.
2. Combine the conditions in the **Logical expression** field using the numbers of the conditions and the Boolean operators AND and OR. For instance: 1 AND (2 OR 3).

The final **and** in the **Conditions** section allows you to specify a condition on an aggregate of the object selected in the **Retrieve** section. Activities and events do not have associated aggregate values.

Beware of literal translations of natural language to logical conditions, because you can get unexpected results. To express what you really mean in an investigation, keep in mind that relations between objects in Nextthink are all related to events in some way. For example, if a device is linked to an application, it is because the application was executed at some point in that device. The system iterates through these relations to return the results of an investigation.

Now consider a case where you want to get a list of the devices that have executed two different applications (e.g. *Internet Explorer* and *Firefox*) within a particular time frame, whose duration is irrelevant to our discussion. You may be tempted to use a logical AND (the default) to combine the conditions of an investigation on devices:

- Condition 1: Application name is *Internet Explorer*
- Condition 2: Application name is *Firefox*
- Logical expression: 1 AND 2

If you run this investigation, the list of devices that you get is always empty. The reason is that any relation between a device and an application ultimately relies on executions and no execution may simultaneously satisfy the two conditions: it is either an *Internet Explorer* execution or a *Firefox* execution, but not both. When the system iterates through these relations, it discards them all because none is matching the two conditions at the same time, as required by the logical operator AND. Hence the empty result.

To properly state the desired query, keep the same conditions but modify a couple of inputs. First, change the logical expression from AND to OR:

- Logical expression: 1 OR 2

In this way, the system keeps the relations that match either the first condition or the second. That is, you get all the devices that executed either *Internet Explorer*, *Firefox*, or both; although you are only interested in the last group.

Last, restrict the output to only those devices that executed the two applications. Add the following aggregate condition at the end of the section:

- Aggregate condition: Number of applications is 2

If you change your mind afterwards and decide to ask for the devices that executed either *Internet Explorer* or *Firefox*, but not both, use the following aggregate condition instead:

- Aggregate condition: Number of applications is 1

Although not useful in the example, the logical AND is still the most common operator to combine conditions. Use it when you want to enforce two compatible conditions at the same time. For instance, to know the devices that use *Internet Explorer* for browsing a particular domain, say *www.example.com*, create an investigation on devices with the following conditions:

- Condition 1: Application name is *Internet Explorer*
- Condition 2: Domain name is *www.example.com*
- Logical expression: 1 AND 2

Time frame

To limit the results of the investigation to a particular range of time, use one of the following options:

Full available period (*start date to end date*)

Do not limit the results. The investigation uses the full range of time available in the Engine, which is stated in the start and end dates. This option is not available for investigations based on activities or events nor for any investigation based on objects that needs to go through activities or events.

On *date*

Limit the results of the investigation to a particular day.

During the last *x* days / hours.

Get the most recent matching results, that is, those that occurred less than the specified number of days or hours ago. Note that, when expressed in days, the time is partitioned in natural days, going from 0h to 23h59. As a consequence, it is not the same to restrict the time frame to the last day (from midnight today until now) than to the last 24 hours.

From *start date and hour* to *end date and hour*

Specify the period limit manually.

Additionally, for specified time frames that span through several days (with the exception of the Full period choice), you can optionally specify a range of hours of interest:

Between *start hour* and *end hour*

Choose a period of interest inside every single day included in the investigation.

Display section

In the Display section you choose the attributes and categories that show up in the columns of the list of results of the investigation for every object, activity or event retrieved.

The attributes and categories are grouped by relevant topics that depend on the kind of item that the investigation retrieves. To select an individual attribute or category, click on its corresponding check box. To select all the attributes inside a topic or all the categories, click the check box of the topic or the general check box for categories.

If only some of the attributes inside a topic are selected, the check box of the topic appear as a solid box instead of as a check mark. If no attribute of a topic is selected, the check box appears unchecked.

Limiting the number of displayed results according to a sorting criterion

To limit the number of displayed items in the list of results of an investigation, use the option that you find on top of the list of attributes and topics of the **Display** section. Choose between:

All results

Display all retrieved items without limit.

The top *x* items ordered by *attribute* ascending / descending

Limit the list of results to the first *x items* in ascending or descending order, according to the specified attribute.

Estimation of the time of execution of an investigation

The time of execution of an investigation depends on the complexity of the investigation and on the size of the database. Aggregate values, large time frames and elaborate conditions add up to the total complexity of an investigation. Based on these parameters, the *estimated run time* indicator in the bottom left corner of the dialog gives you a hint of the total execution time of the investigation that you are editing.

The indicator has three levels: low, medium and high. These levels are expressed graphically by means of three bars. One blue bar meaning low run time, two yellow bars meaning medium run time and three red bars meaning high run time. For small databases, the difference in the time of execution between a low run time investigation and a high run time investigation is hardly noticeable by the user. On the other hand, for big databases, the difference may be much more appreciable.

If you hover the mouse over the estimated run time indicator, a tool tip gives you some instructions on how to reduce the time of execution of the investigation.

Navigating through the results of an investigation

After executing an investigation, you are presented with a list of all the items that matched your query conditions. This is the **List** view of the Finder.

The list displays all the fields and aggregates that you selected when you edited the options of the investigation.

Sorting the results

Order the results in the **List** view according to the value of one of the displayed fields by clicking its corresponding column header. The arrow to the right of the column name indicates if the sorting is made in ascending (arrow up) or descending (arrow down) order. Click the column header again to change the direction of the arrow.

By default, results are sorted according to the values of the first column in ascending order. You can click on any other column header to sort the results in

other ways.

Changing the time frame


The **List** view displays the time frame that applies to the given results of the investigation in the top-center part of its own tab. To change the time frame of the investigation, click the calendar icon that appears to the right of the current time frame. A dialog very similar to the Time frame section of the investigation designer shows up. Set the new desired time frame and click **Apply**.

To come back to the original time frame of your investigation, click the calendar icon and then push the button **Reset**.

If you selected a limited time frame such as a particular day, you can also navigate easily with the arrows you find in both sides of the calendar icon. Just press the arrow to the right to move to the next available day, or the arrow to the left to move to the previous day.

Setting the platform

From the **List** view, filter the results of an investigation according to platforms at any time:

1. Click the platform icons at the top of the **List view**, , and a dialog to select the platforms shows up.
2. Tick the check box for every platform that you want to include in the results.
3. Optional: To go back to the platforms originally selected by the investigation, click **Reset**.
4. Click **Apply** to filter the results according to the selected platforms.

Adding and removing display fields

To quickly add more fields to the ones displayed in the **List** view or remove some of the fields:

1. Right-click anywhere in the column headers of the list of results (the top part with the names of the columns). A context menu shows up.
2. Hover the mouse cursor over the option **Add or remove columns**. The whole set of available fields appears next to the menu.
3. Tick the boxes that correspond to the fields that you want to add and untick those that you want to remove.

4. Click **Apply**.

To quickly remove a single column, right-click the column header and select **Remove column** from the context menu.

Drilling-down

Drilling-down to other items from your list of result items is one of the most powerful tools that you have for navigating through the results of your investigations. Drilling-down lets you get items related to the items in the list of results while keeping the context of your investigation, that is, enforcing the time frame and the conditions of the original investigation.

A drill-down is actually a quick investigation on objects, activities, or events that are related to a selection of the results of a previous investigation. For instance, imagine that you execute an investigation on devices, looking for those devices that executed the Nextthink Finder yesterday. You get a list of devices as a result. Imagine now that you want to know the users that executed the Finder yesterday from one or several of those devices. You can get the list of those particular users by drilling-down from the results of your previous investigation. Note that drilling-down keeps the conditions and the time frame of the original investigation, that is, the execution of the Nextthink Finder yesterday.

To drill-down from a list of results of an investigation:

1. Execute the investigation of your choice.
2. Select one or more of the items in the **List** view.
3. Right-click the items selected. A context menu shows up.
4. Select the option **Drill-down to** and choose a type of item. Items are classified into:
 - ◆ **Objects**
 - ◆ **Activities**
 - ◆ **Events**
5. Choose one class of items and then a particular type of object, activity or event. Only those types of items that can be related in some way to the items in the list of results are eligible for drilling-down.
 - ◆ If the items in the list of results are filtered by platform, the drilling-down shows only those items which are compatible with the selected platform.
 - ◆ In the case that you selected multiple platforms, the drilling-down shows all those items which are compatible with any of the selected platforms.
6. A new tab with the list of results for the drill-down opens.

The items that you can select for drilling-down depend also on the platform of the item you drill-down from. For instance, you cannot drill-down to printers from a Mac OS device, because the Mac OS platform does not support printers.

One-click investigations

One-click investigations are similar to drill-down investigations, except for the fact that they do not keep the context of the previous investigation.

For instance, to go on with our previous example, imagine that you are navigating the **List** view of an investigation that returns all the devices that executed the Nextthink Finder yesterday, and that you want to know all the users of a particular device. Drilling-down to users returns only those users who executed the Finder yesterday on that device. On the other hand, a one-click investigation on users returns all the users who have ever been seen in the device, regardless of what they were doing or when.

To perform a one-click investigation from the list of results of a previous investigation:

1. Execute the investigation of your choice.
2. Select one or more of the items in the List view.
3. Right-click the items selected. A context menu shows up.
4. Select the option **One-click investigation** and retrieve all the items of a particular class. Choose among:
 - ◆ **Retrieve all objects**
 - ◆ **Retrieve all activities**
 - ◆ **Retrieve all events**

Note: for binary objects, specify first if you want to retrieve items related to the binary itself, or to the executable or the application to which the binary belongs. Similarly, for executable objects, choose first if you want to retrieve items related to the executable itself or to the application to which the executable belongs.
5. Select a particular type of object, activity or event. Only those types of items that can be related in some way to the items in the list of results are eligible for a one-click investigation.
 - ◆ If the items in the list of results are filtered by platform, the one-click investigation shows only those items which are compatible with the selected platform.
 - ◆ In the case that you selected multiple platforms, the one-click investigation shows all those items which are compatible with any of the selected platforms.

6. The Finder opens a new tab with the list of results for the one-click investigation.

Again, similarly to what happens with drill-downs, the items that you can select when you do a one-click investigation depend also on the platform of the *one-clicked* object. For example, you cannot retrieve all events related from a Mobile device because Mobile devices do not support events.

Saving your modifications

When you change the time frame or the displayed fields, or you drill-down, or do a one-click from the **List** view of an investigation, the system is actually executing a different investigation from the original one.

To save the new investigations that you create by applying modifications to the **List** view, click the floppy disk icon at the top right of the view.

Getting a graphical representation of the data

The **List** view gives you a plain text representation of the data stored in the Nextthink database. While this is perfect if you want to have a list with the exact values, it can be difficult for a human to get an insight of what is actually happening inside your IT infrastructure with just a textual representation.

To get a graphical representation of the results in the List view, click one of the buttons in the top-left corner of the List view:

Network activity

To visualize network connections.

Web activity

To visualize web requests.

Local activity

To visualize local program executions.

The visualizations are computed within the context of your investigation. Therefore, not all three visualizations are present for all investigations. A visualization is available only if the context contains relevant information for it.

Related tasks

- Executing an investigation
- Editing the options of an investigation
- Creating an investigation

- Viewing network connections
- Viewing web requests
- Viewing executions

Comparing the properties of users and devices

One option to see and compare the properties of users or devices is to create appropriate investigations and display as many of their properties as desired, visually comparing the values in the list of results.

A better way to see how a property of a user or device compares to the same property of other users or devices is to use the **Properties** tab of the *user view* or of the *device view* in the Finder. Open the user view or device view of a particular user or device and click the **Properties** button. The **Properties** tab presents in a single page all the relevant attributes of a user or device conveniently grouped.

Device sections	User sections
<ul style="list-style-type: none"> • Hardware • Network • Startup • Operating system • Local drives • Categories 	<ul style="list-style-type: none"> • Active directory • Last user activity • Categories

Some of the properties have a small bars icon to the left of their name. The small bars mean that the property can be compared with the value of the same property in other users or devices. Clicking the name of a comparable property opens a bar chart in which the heading of each bar is one (or a range) of the possible values for that property and the length of the bar indicates the number of total users or devices that share that same value. The actual number of devices that share the value is also shown as a figure to the right of the bar. The bar whose value matches the value of the property of the currently selected device in the device view is highlighted in the chart.

Since the available properties of a device depend on its platform, the Finder lets you compare the properties of a device only with those other devices that share the same platform. With respect to users, you can just compare the categories to which a user belongs.

In the case of devices, the bar chart shows thus how the values of certain properties are distributed among the devices in your network. This is very useful to assess particular problems of a device. For instance, if a user complains because his laptop takes a long time to boot, you can click the property **Average boot duration** in the properties page and compare the boot duration of the laptop of the complaining user with the average boot duration of all other computers. If most of the other computers boot in a shorter time than the given laptop, you can conclude that the user really had a reason to complain. You may then look at the hardware properties of the laptop and analyze whether it needs a hardware upgrade.

To show a list of the users or devices that contribute to the length a bar in the bar chart, double-click the bar or right-click on it and select **Drill-down**. The drill-down is equivalent to launching an investigation on devices with that property value.

Selecting a group of users or devices for comparison

By default, clicking a small bars icon compares a property of a user or device with the same property of all other users or devices in the database. To limit the group of users or devices that take part in the comparison, use the **Compare with** tool. This tool is found in the top right corner of the **Properties** tab in both the user view and the device view.

To select a group of users for comparison with the current user, the **Compare with** tool makes use of categories. Thus, all users that share the same category keyword can form a group. In their turn, devices can be grouped by entity as well as by category keyword.

To limit the group of users used in comparisons:

1. In the **Compare with** tool, select **users with category** from the list instead of the default **all users**. A selection box appears to the right holding the list of all user categories. Another selection box appears below with the text **and same keyword**. To the right of this last box, find the value of the keyword for the selected category and for the current user within parentheses.
2. Select a category from the list.
3. Select the category keyword that defines the group.
 - ◆ If you want to compare with the group of users that share the same keyword as the current user, leave the default value **and same keyword** and you are done.

- ◆ If you want to compare with another set of users, choose the option **and keyword** instead of the default **and same keyword** in the selection box. Another selection box appears to the right, holding the list of all available keywords for the selected category.

1. Select the keyword that defines the comparison group of users from this last box.

To limit the group of devices used in comparisons by category keyword, follow the instructions given above for users. The method is basically the same: just select **devices with category** in the **Compare with** tool. Limiting the comparison group by entity is also very similar:

1. In the **Compare with** tool, select either the option **devices with same entity** or **devices with entity**.

- ◆ If you choose **devices with same entity**, the comparison group is formed by those devices that share the same entity as the current device. The name of the entity is displayed within parentheses to the right of the selection box.

- ◆ If you choose **devices with entity**, another selection box appears to the right, holding the list of all available entities.

1. Select an entity from the list to define the group of devices for comparison.

Remember that, in any case, the Finder compares the properties of a device with devices that share the same platform only.

Related tasks

- Graphically observing the activity of users and devices

Visualizing system activity in the Finder

Getting a quick overview

Get a glimpse of recent happenings in your setup thanks to the *Quick views* of the Start page. Quick views summarize important information and let you perform frequent tasks, such as executing the most recently used investigations or inspecting services in detail. By default, the Start page displays the Quick views at the bottom of its main space, which is shared with the Search tool. Thus, launching a search effectively hides the Quick views, which are replaced by the results of the search. To get the Quick views back, erase the contents of the Search box.

Quick views are disposed horizontally in the screen as individual boxes. Scroll the Quick views with the help of the arrows placed on the left and right sides of the views to see all the boxes.

Recent alerts

The **Recent alerts** box highlights the alerts on devices that were triggered during the last 24 hours. The box displays the name of the alert along with the number of devices that generated the alert inside a red circle.

To analyze the alert in detail, click the name of the alert in the box for getting the list of impacted devices.

Services with threshold violations

The **Services with threshold violations** box shows a list of services ordered by the gravity of the violation (depending on whether the service crossed either the error or the warning threshold) and the number of devices impacted during the last 24 hours. For each service, the list displays the name of the service and, inside a red circle, the number of devices that attempted to connect to the service but found an issue.

To analyze the service in detail, click the name of the service in the list for opening the Service view.

Recently used investigations

The **Recently used investigations** box holds a list of the last five investigations that you executed in the Finder. To execute again any of the investigations in the list, click the name of the investigation.

Only named investigations are stored in the list of recently used investigations.

Graphically observing the activity of users and devices

Overview

To see at a glance the recent activities or the detailed properties of a particular user or device, open either their *user view* or *device view* in the Finder. Both the user and the device views have a **Timeline** tab and a **Properties** tab:

- Select the **Timeline** tab to explore the activities of a user or device in chronological order.
- Alternatively, select the **Properties** tab to display detailed information about a user or device.

By default, the device and user views open the **Timeline** tab. Note however that mobile devices do not have a **Timeline** tab, so the device view of mobile devices display only the **Properties** tab.

To open the user view or the device view of a particular user or device, either:

- Look for the user or device in the search box of the **Start** page and click the name of the user or device in the results of the search.
- From the list of results of an investigation based on users or devices, right-click the entry of the user or device and select **Display user view** or **Display device view**, or double-click the entry of the user or device, or select it and press **Enter**.
- From any of the other graphical views of the results of an investigation (**Network activity**, **Web activity** or **Local activity**) that display users or devices, right-click the name or the icon of a user or device and select **Display user view** or **Display device view**.
- From the user view itself, open the device view of any of the devices listed in the **Devices** section of the **Timeline** tab, or listed in the **Last user activity** section of the **Properties** tab, by clicking their name.

- Likewise, from the device view, open the user view of any of the users that interacted with the device, displayed in the section **Users** of the **Timeline** tab, by clicking their name.

At the top of the view, get basic information about the selected object:

User view	Device view
<p>Name The name of the user.</p> <p>Type The class of user: local, domain or system.</p> <p>First Seen The first time of recorded user activity.</p> <p>Last Seen The last time of recorded user activity.</p>	<p>Name The name of the device.</p> <p>Platform icon A pictorial representation of the platform of the device: Windows, Mac or mobile.</p> <p>Entity The base node in the hierarchy to which the device belongs.</p> <p>Last IP address The IP address of the device during its last recorded connection.</p> <p>Last Seen The last time of recorded device activity.</p>

Below this basic object information, find the buttons that let you switch between the **Timeline** and the **Properties** tabs. When selecting the **Properties** tab, a comparison tool appears to the right of the basic object information. The rest of this article is dedicated to the **Timeline** tab, while the article on comparing the properties of users and devices focuses on the **Properties** tab.

To refresh the view, click the button with a circular arrow placed to the far right of the tab selection buttons. Refreshing the view is particularly useful when it is open for a long time and you want to see the last activity of a user or device.

Exploring activities in the timelines

The **Timeline** tab displays in fact several timelines grouped by sections. While the actual sections and their content depend on the type of object observed (user or device), the techniques to explore the timelines remain essentially the same.

To know the time scale of the timelines, find a ruler at the top of the view that divides the horizontal space in equal parts. Each subdivision of the ruler corresponds to a time interval of the recent history of the user or device under

examination. Date and time labels in the ruler indicate the precise moment associated to a subdivision mark. In accordance with the ruler, an activity or event in the timelines found by following down a vertical line from a particular subdivision occurred during the time interval associated to that subdivision.

Hover the mouse cursor over a timeline with data and keep it there for a moment. A kind of structured tooltip eventually shows up. The tooltip summarizes the activities and events related to the timeline that happened during the time slot under the mouse cursor. A vertical and a horizontal dashed lines, crossing at the timeline slice pointed by the mouse cursor, show up shortly after the tooltip to help you locate the time interval in the ruler and the title of the timeline.

To investigate further what happened during a timeline slice, right-click the timeline at the point of interest. A context menu displays a list of options that let you open different views or drill down to related items, depending on the particular timeline. To directly drill down to the related main objects or events instead, double-click the timeline .

By default, the **Timeline** tab displays the last 24 hours in the history of a user or device.

Navigating through history

To the left of the date and time ruler, click the button with a triangle pointing to the left to go back in time. Likewise, click the button to the right of the ruler that depicts a triangle pointing to the right to go forward in time. For displaying data further in the past or closer to the present, the ruler and the timelines scroll right or left accordingly, following the opposite direction of the arrow clicked.

Alternatively, hover the mouse pointer over the ruler. The pointer turns into a double-headed horizontal arrow. Click and drag the pointer to the left to go forward in time. To go back in time, click and drag the pointer to the right. The ruler and the timelines scroll as you drag the mouse pointer.

The available history is limited by the amount of events recorded in the in-memory database of the Engine. The Finder stops scrolling to the past once you reach the time of the oldest event in the database. For completeness, the Finder lets you scroll a few hours into the future. It does not make much sense to go beyond the present time though, as the future is naturally empty of data.

Zooming

The default settings of the **Timeline** tab let you see the last 24 hours of a user or device. At that zoom level, every subdivision in a timeline represents a time interval of 30 minutes. With this granularity, two events separated by ten minutes, for instance, may reside in the same time slot, giving the appearance of simultaneity.

To know which event happened first, select an area surrounding the apparently simultaneous events and zoom in:

1. Click the part of the timeline located immediately before the events of interest and keep the mouse left button pressed.
2. Drag the mouse cursor over the events of interest and release the mouse button as soon as you have covered them with a rectangular selection area.
3. Click the magnifying glass with the plus sign that is placed in the top right corner of the timelines or press **Enter**.

This *zoom in* button is enabled only when you have selected an area in the timelines. It also gets disabled when you reach the maximum allowed resolution (one second per subdivision).

Some timelines related to events also propose an option to zoom in in their context menu. As an alternative to the zooming method proposed above, right-click the timeline and select **Zoom in on events** when available.

To zoom out to the previous level, click the magnifying glass with the minus sign in the top right corner of the timelines or press **Backspace**. The *zoom out* button is enabled until you reach the maximum time span allowed (7 days).

To go back to the default 24 hours view, click the house icon placed to the left of the two magnifying glasses.

Timeline sections of the user view

In the timelines of the user view, find events and activities related to the devices with which the user interacted, the print jobs that the user started and the services that the user accessed.

Remember that timelines are actionable. Right-clicking a point in the timeline brings up a context menu with drill-downs and other options to jump to information related to the data in the timeline.

Applies to platforms:
Devices

For every active device linked to the user, find one or several timelines associated to it. The information displayed in the timelines depends on the platform of the device. For Windows or Mac devices, a main timeline groups all the information available. Click the plus icon to the left of the name of the Windows or Mac device to expand the main timeline into its individual components. Mobile devices display the times of synchronization with the server.

Windows or Mac	Mobile
<p>Device alerts Occurrences of investigation-based alerts.</p> <p>Errors Applications not responding or crashing, bluescreens and hard resets.</p> <p>Warnings Notifications of high cpu load, high memory usage, or a big number input and output operations or page faults.</p> <p>Interaction Times when the user was active on that device (with the keyboard or the mouse), in addition to system boots and user logons.</p>	<p>Exchange ActiveSync synchronization Synchronization of the mobile device with the Exchange server.</p>

Although Windows and Mac devices share the same timelines, note that all the information available for Windows devices is not yet available in Mac devices. Namely, Mac devices display no warnings and only *hard resets* as errors.

For device events to appear in the user view, they must be related to some user interaction with the machine.

Printers

For each printer, find the print jobs that the user has sent. Click the plus icon to the left of the name of the printer to break down the print jobs by device. Each print job appears then on a different timeline depending on the device that the user employed to send the print job.

Services

See the activity of the user in relation to the services that you have defined. Click the plus button to the left of the name of the service to break down the activity by device. Depending on how you defined the service, you can further break down to the activity of the executables that compose the service.

Timeline sections of the device view

In the timeline, you can quickly detect whether the computer generated any alert, experienced any error or warning, had new software installed, connected properly to networked services, etc. This information is presented in different sections.

Note that the timeline is not available for the Mobile platform and that not all its sections are available or complete for the Mac OS platform. Namely, for Mac OS, the Errors section displays only hard reset errors, whereas the Warnings section as well as the Web services section do not exist.

From top to bottom, the timeline of the device view displays the sections detailed below.

Applies to platforms:

Alerts

There are two separate sections:

- Global alerts.
- My alerts (user-defined alerts).

Each defined alert has its own timeline. Occurrences of the alert are marked in the timeline, graphically showing their start time and the duration. For the sake of clarity, only alerts that have been triggered during the selected time frame are displayed.

To see the exact time of triggering and the duration of an alert, hover the mouse cursor over the occurrence of the alert. If more than one occurrences of the alert overlap, the hovering tooltip gives you a list of all the occurrences.

To see a list of all the devices that triggered an alert, right-click the mark of the alert in the time-line, choose an occurrence if more than one is available and select **Show Alert**.

Errors

Signal errors in the device, such as application or system crashes. The error is shown in the timeline as a red circle with a number inside. The number inside the circle is bigger than one if more than one error condition overlap in the timeline. Hovering the mouse over the circle gives you a summary of the reason for the error (or the reasons, in the case of overlapping errors).

Warnings

Warnings are represented in the timeline as small boxes. The brightness of the color of the box indicates the severity of the warning. The brighter the color is, the more severe is the warning.

Hovering the mouse cursor over a warning displays a summary of the reasons for the warning. For example, when hovering over warnings on applications using too much cpu or memory, a tooltip gives you a list of the applications that contribute the most to consumption of these resources.

Activity

In the **Activity** section, you find information about momentary activities, such as the detection of new binaries, print jobs, system boots, user logons and package and patch installations and uninstallations. You find as well information on lasting activities such as executions and connections.

Momentary activities are shown in their own timeline as blue circles with a number inside that indicates the number of overlapping events, similar to the red circles used for displaying errors. Lasting activities, in turn, are shown as blue squared boxes in the timeline, where the brightness of the color indicates the level of the activity (number of executions or connection traffic), similar to the boxes that are used to display warnings. As usual, if the system did not perform any activity of a certain type the activity is not shown at all, instead of displaying an empty timeline.

For every momentary activity, hovering the mouse cursor over the blue circle gives you a summary list of the causes for displaying the activity. For instance, hovering over a **New binaries** occurrence in the timeline displays a list of the binaries whose execution has been detected for the first time at that precise moment. Right-clicking in a blue circle of a momentary activity lets you choose among different options depending on the type of activity.

For lasting activities, that is **Connections** and **Executions**, hovering the mouse over a blue box yields:

- For **Connections**, the amount of traffic registered during the time span of the box.
- For **Executions**, the number of processes run on the time span of the box.

You can drill-down from a box of a lasting activity to the list of individual connections or executions that make it up by right-clicking in the box and selecting **Show connections** or **Show executions**. Connections have an additional option **Show network activity** that lets you navigate directly to a Network activity view and specify the metric to see in it (traffic in, traffic out, failed connections, etc).

In the **Activity** section, yellow color in the timeline warns you about administrator activity. A warning message notifies the use of administration privileges when you hover the mouse cursor over an activity timeline with yellow color. Two kinds of activities use a yellow display when they are carried out by users with administration privileges: **User logons** and **Executions**.

- When a user logs in to a device with administration privileges, the circle representing the user logon activity is no longer blue, but yellow.
- When a program is run with administration privileges, the blue boxes that show the executions are crossed by a yellow line to warn that at least one had admin privileges.

Network services

For every defined network-based service, you see a timeline indicating the status of the connections of the selected device to the service. Network connections to the service are displayed again as blue boxes. If any connection problem is detected, the blue boxes are crossed by a yellow line to indicate a warning and by a red line to indicate an error.

To see a summary with the statistics of the connections to the service (total traffic, number of connections, failed connections, response time, etc), hover the mouse over the desired box in the timeline. Additionally, you get a summary list of the errors and warnings that happened during the period delimited by the box, if any.

To open the Service view, click the name of the service at the beginning of the timeline or double-click a box in the timeline. There you find detailed information

about the service for the last 24 hours.

Finally, you can also navigate to the Network activity view of the connections to the service from the timeline by right-clicking on any box and selecting **Show network activity**. Double-click in the box, as with connections in the **Activity** section.

Web services

If you installed the **Web & Cloud** module as an addition to the Nextthink Platform, you find a **Web services** section in the device view dedicated to web-based services. This section is very similar to the one dedicated to network-based services.

By hovering the mouse cursor over the boxes in the timeline, you get the statistics about the web-based service: traffic, requests, type of responses, average response time, etc.

To open the Service view, click the name of the web-based service at the beginning of the timeline or double-click a box in the timeline. To navigate to the Web activity view, right-click a box in the timeline and select **Show web activity**.

Users

At the lower part of the device view, you find the timelines that measure the interaction of users with the selected device. There is a timeline for each user that interacted with the machine and the account name of the user is displayed to the left of the timeline. Hovering over each box in the timeline gives you the total duration of the interaction.

For privacy reasons, measurement of the interaction time of the user with the computer can be disabled. If user interaction measurement is disabled, the **Users** section is omitted in the device view.

Click the name of a user to open the corresponding *User view*.

Related tasks

- Comparing the properties of users and devices

Related concepts

- Device

Observing service performance

Analyzing service status in real-time

To analyze the status of a service in real-time for the last 60 minutes and the last 24 hours, open the Service View in the Finder:

1. Go to the **Services** section in the accordion of the Finder.
2. Double-click the name of the service.

An overview of the service is displayed in a new tab. The overview is divided into two differentiated parts:

- The upper half part, which shows the metrics that measure the performance of the service.
- The lower half part, which shows the evolution of the selected metric over time.

The metrics that measure the performance of the service are, in their turn, divided into two rows. The first row gives a short-term view of the service for the last 60 minutes and the second row gives a longer-term view for the last 24 hours. For each metric, you get the current value over the period of 60 minutes or 24 hours and the difference with respect to the previous period. For instance, if the time now is 16h40 (measured with a 10 minute resolution), the last 60 minutes span from 15h40 to 16h40 and the difference is computed with respect to the time span from 14h40 to 15h40.

An indicator arrow accompanies the difference value. The arrow points up if the current value is bigger than the previous value and it points down if the current

value is smaller than the previous value. In addition, the color of the arrow indicates if the variation on the value of the metric means an improvement or a degradation of the service, because bigger does not necessarily mean better. For instance, an increasing number of failed connections is indeed a bad sign for a service. The arrow looks therefore green when the service improves, red when the service degrades and blue if the metric is merely informative and neutral with respect to the quality of the service.

Evolution of service metrics over time

Right after you create a service, all its metrics have a zero value and the two rows that display the metrics (the first for short-term metrics and the second for long-term metrics) are both labelled **Last 10 minutes**. This is a consequence of the way in which Nextthink continuously monitors services.

In the lower half part of the service overview, below the figures of the metrics, you find a bar chart that shows the evolution of the service with time. The bar chart graphically displays the values of the selected metric, as measured in intervals of one hour for the last 24 hours. To change the selected metric, click the name or the value of the metric that you wish to display. A pointer arrow zooms in the selected metric and singles it out from all the other metrics.

The bar chart is a composed chart. By default, the top bar chart shows the total values of the metric during the last 24 hours and the charts below break down the total into the partial values that correspond to each entity in your hierarchy. You can change the default behaviour and focus on the values of a particular entity. To focus on the results of an entity, you can either:

- Click the name of the entity at the head of its corresponding bar chart.
- Select the entity from the list placed at the top left corner of the tab window, preceded by the legend **Display data for**.

When you focus on an entity, the top bar chart shows the values of the metric for that entity only. The bar charts below, when present, show the individual devices belonging to the entity and whether they contributed to the value of the metric or not during a particular hour. Therefore, the bar charts for individual devices are only present when the selected metric counts the number of impacted devices. In this case, bars do not denote a quantity level, but just membership of a particular device to the group of impacted devices. If the selected metric computes anything other than a number of devices, such as an average of connections or network traffic, there are no bar charts for the individual devices. Instead, you

find the text **no device data in this mode**. The metrics that count devices and, consequently, show individual device data are the same for both connection-based and web-based services:

- Devices with issues.
- Devices using service.
- Application crashes (this metric does not count the number of crashes but the number of devices with application crashes).

Similarly to the indicator arrows that compare the current value of a metric to its previous value, the bar charts also use a color code for quick visual recognition. A red bar indicates an error condition in one or more of the concerned devices, yellow means warning and blue is used for neutral metrics. The metric **Devices with issues** may combine error and warning conditions in a same bar. The amount of red and yellow in the bar is then proportional to the number of devices with errors and warnings respectively. A single device may also have yellow and red combined in its own bars, meaning that the device generated both errors and warnings on the specified hours.

In the bar chart, the rightmost interval corresponds to the current hour. The interval of the current hour is divided into sub-intervals of 10 minutes each. The bar that shows the value of the selected metric for the current hour displays the partial results of the metric from the beginning of the hour up to the last 10 minutes sub-interval. The included sub-intervals of 10 minutes are highlighted in the time axis.

Placed to the right of the current hour interval, you find a bar that groups the total value of the metric for the last 24 hours. Contrary to all other bars in the chart, the bar with the total value grows horizontally. Each row in the bar chart displays its own totals, so you can visually compare their values. Rows can be ordered with respect to their total value for the metric. To sort the rows by their total value in the last 24 hours:

1. Find the arrows below the header of the column **totals**.
2. Click the arrow pointing up to sort the rows in ascending order.
Alternatively, click the arrow pointing down to sort the rows in descending order.

You can also sort the rows in alphabetical order or look for a particular entity or device in the bar chart. To look for a particular entity or device:

1. Find the text box with the magnifying glass placed to the left of the bar chart, on top of the names of the entities or devices.

2. Type in a part of the name of the entity or the device that you wish to find.

The bar chart displays only the entities or devices containing the exact sequence of characters typed in. To the left of the text box, there are a couple of arrows that are very similar to the arrows in the **totals** column. You can click the up arrow to arrange the displayed entries in alphabetical order or the down arrow to display the entries in reverse alphabetical order.

From the service overview, you can launch contextual investigations related to the service. Contextual investigations and their visualizations let you examine in detail the connections or web requests accessing the service and the activity of devices using the service.

Bar chart tooltips

Hovering the mouse cursor over a one hour interval in the bar chart, even when no bar is present in that interval, shows up a small window with the complete summary of the values of the metrics for the selected hour.

The currently selected metric is highlighted in the window. In addition to the metrics, the summary breaks down the number of devices with issues into devices with specific errors and warnings. For instance, if there is an application crash in two different devices during the selected hour, you see the message *2 with application crashes*. Error messages are colored in red and warnings in yellow.

See below the list of possible errors and warnings:

Type	Common	Connection-based	Web-based
Errors	with application crashes	with connection failures lasting more than a minute	with number of 5xx requests over 3 times last week average

Warnings		with response time over 3 times last week average	with average request duration over 3 times last week average
			with number of 4xx requests over 3 times last week average
			with number of 3xx requests over 3 times last week average

For more information about service errors and warnings see [Service errors and warnings](#).

Network activity and Web activity

To see the individual connections of a connection-based service, click the **Network activity** button, placed on top of the main window of the service and to the right of the **Overview** button, which is pressed by default. The main window of the service displays then a graphical view of all the service connections for the last 24 hours instead of the service overview. To learn more about how to interpret the graphical view of connections, see the chapter on [Viewing network connections](#).

Similarly, to see the web requests of a web-based service, click the **Web activity** button that replaces the Network activity button of connection-based services. You get a graphical view of all the web traffic related to the service for the last 24 hours. See the chapter on [Viewing web requests](#) for an explanation on how to interpret the graphical view of web traffic.

Drill-downs

In addition to the buttons of **Network activity** and **Web activity**, you can also launch investigations and visualizations of connections and web requests from the bar chart of the service overview. Double-click a bar in the bar chart to launch a contextual investigation or graphical visualization that depends on the metric selected and is restricted to the entity or device at the head of the row where the bar is placed and the interval of one hour that delimits the graphical bar. For example, if you double-click a bar of the default entity *empty* whose level indicates the number of devices using the service from 12h00 to 13h00, you get a list with all the individual devices belonging to the entity *empty* and making use of the service during that period. As another example, if you double-click a bar

that indicates failed connections, you get a visualization of the individual failed connections.

Double-clicking a bar gives you a default investigation or visualization. Alternatively, you can right-click a bar to choose the investigation or visualization that you want to see. When double-clicking or right-clicking a bar in the bar chart of the service overview, results are displayed in a new tab window.

When you focus on an entity by clicking its name in the bar chart or choosing it in the **Display data for** list, you see data of individual devices in the bar chart. Clicking the name of a device opens the device view, which shows detailed information on the activity of the device and is explained in the chapter about observing the activity of users and devices.

Related tasks

- Analyzing service quality
- Creating a service
- Following the evolution of a service
- Hierarchizing Your Infrastructure
- Viewing web requests
- Viewing network connections

Related concepts

- Service
- Hierarchy
- Entity

Related references

- Real-time and consolidated service data

Viewing network connections

To visualize network connections in a graphical way, use the *Network activity* view. The Network activity view relates all the objects that participate in a network connection.

To open the Network activity view:

1. Execute an investigation based on connections or on any of the objects that participate directly or indirectly in a network connection: device, user, application, executable, binary, port or destination.
2. From the list of results, click the **Network activity** button placed at the top of the list.

You can also open the Network activity view from other contexts such as the device view or the services view. In any case, an underlying investigation is generated for you, displaying the Network activity that corresponds to that investigation.

Interpreting the Network activity view

The Network activity view arranges objects in five columns, one per class of object that participates in a connection: device, user, binary, port and destination (applications and executables participate indirectly in a connection through binaries). Straight lines connect objects in contiguous columns whenever the linked objects took part in a network connection. The thickness of the lines indicate a quantity that depends on the kind of information that you selected in the **Display** choice list that is found in the top left corner of the panel. By default, lines display the total traffic, so the thicker the line is, the higher the amount of traffic exchanged during the connection. But you can select to display the number of failed connections, the average response time, the bitrate of the connection, etc. Hovering the mouse over a line gives you the exact quantity of the information selected. A dashed line indicates a zero amount of the kind of information selected; for instance, you may select to display the total traffic and have a very thick line joining a set of objects and then select to display the number of failed connections and have a dashed line instead, because all connections were successful.

Grouping objects in the columns of the diagram

When a column contains many objects, the Finder collapses them into groups of objects. You distinguish collapsed objects from single objects by the small plus sign that shows on the icon of the collapsed objects. To expand a group of collapsed objects, click the plus sign. If a dotted line appears between expanded objects, that means that they share common traits and they are suitable for collapsing. Click the dotted line and the objects linked by the line will collapse. Alternatively, right-click on an object and select **Collapse** or **Expand**. The right-clicking option allows you to force a collapse of objects even when no dotted line links them. As a special case, binary objects can collapse into executables and applications and be displayed as such in the column dedicated to binaries. Groups of devices and ports can additionally display a star on their

respective icons. For a group of devices, the star denotes that they all belong to a single entity, which is a special kind of category. In the case of ports, the star indicates that the icon represents a group of scanned ports. You cannot expand scanned ports to analyze them individually. The group of external destinations is represented by an icon with the shape of a cloud in the column dedicated to destinations. Similarly to a group of scanned ports, the group of external destinations cannot be expanded to individual destinations.

If the number of objects in a column exceeds the vertical space available to show them, an arrow above the column and an arrow below the column help you reach the objects that lie out of bounds. Hover the mouse cursor over the arrows to navigate up or down the objects in the column or click the arrows to navigate quickly.

Navigating through paths and objects

When you click on a line of the Network activity joining two objects, a full path from device to destination is highlighted based on your selection. Right-click the path to drill-down to related objects or activities or execute a related one-click investigation, as you would do from the list results of an executed investigation. You can select several paths at the same time by pressing the **Ctrl** key while you click the paths.

If the Network activity corresponds to an investigation based on objects and not directly based on connections, a list of objects from the results of the investigation appears to the left of the diagram. For instance, if you execute an investigation on devices and then select the Network activity view, the left hand side of the diagram displays a list of the devices included in the results of the investigation. The list of objects interacts with the displayed lines of the Network activity diagram. If you select a path in the Network activity diagram, the objects that took part in the selected connections are highlighted in the list. The reverse is also true: if you select a specific object from the list, paths representing connections in which the object took part are highlighted in the Network activity diagram. Again, you can select several paths or several objects at the same time by pressing the **Ctrl** key while clicking the lines or the names of the objects. Right-click the name of an object to get the usual drill-down and one-click investigation options associated to the object.

The bar chart of time limited investigations

If the Network activity view relates to an investigation limited in time (full period investigations and investigations specifying **Between** hours are excluded), a bar chart spanning the period of the investigation appears below the diagram of

columns. The height of a bar represents a quantity that depends on the type of information selected in the **Display** choice list, in the same way as the thickness of a line in the diagram does. The value of a bar is valid within the time that corresponds to its width. Hover the mouse over a bar to display the numeric value represented and the time interval that the bar spans. The Finder automatically computes the width of the bars and scales them to fit the time frame of the underlying investigation:

- For a maximum time frame of 7 days, a bar represents 2 hours of data.
- For a minimum time frame of 30 minutes, a bar represents 30 seconds of data.

The bars in the chart also interact with the path lines of the Network activity diagram. Click a bar and the associated paths will be highlighted in the diagram. Click a line of the Network activity diagram and the corresponding sections of the bars will be highlighted in the bar chart. Once again, you can select several lines or several bars by clicking them while you press the **Ctrl** key. Right-click a bar or a group of selected bars to drill-down to related objects or activities or to execute one-click investigations.

Zooming in and out

To limit the number of lines in a diagram to those that correspond to one or more bars in the bar chart, use the **zoom in** icon (the magnifying glass with a plus sign) placed on the top right corner of the Network activity diagram. Selecting one or more bars in the bar chart enables the **zoom in** icon. Click the **zoom in** icon and only the lines that relate to the bars selected will remain displayed in the diagram. After zooming in, come back to the original time frame by clicking the **zoom out** icon that lies to the right of the **zoom in** icon.

In a similar way, you can reduce the number of paths in a diagram to those selected using the zoom. Select one or more paths in the diagram and click the **zoom in** icon. Only the selected paths and their related objects remain displayed in the diagram. Click the **zoom out** icon to come back to the previous zoom level.

Limits of the diagram

If the investigation involves a big amount of connections, the Network activity view may not be able to display all the corresponding paths. When the limit of ten thousand paths is exceeded, a warning icon appears in the top right corner of the diagram, to the left of the zoom icons, meaning that only partial results are shown in the diagram.

To see the Network activity diagram in full screen mode, click the growing square icon that is placed to the right of the zoom icons. This is specially useful in diagrams with lots of connections to better distinguish the different paths. To come back to the original view of the diagram, click the shrinking square icon that replaces the growing square icon in full screen mode.

Related concepts

- Connection

Related references

- Incoming traffic measurement

Viewing web requests

If you added the **Web & Cloud** module to your installation of the Nextthink Platform, you can visualize web requests in a graphical way with the *Web activity* view. The Web activity view relates all the objects that participate in a web request in much the same way that the Network activity view displays network connections, since a web request is a special kind of connection.

To open the Web activity view:

1. Execute an investigation based on web requests or on any of the objects that participate directly or indirectly in a web request: device, user, application, executable, binary, port or destination.
2. From the list of results, click the **Web activity** button placed at the top of the list.

You can also open the Web activity view from other contexts such as the device view or the web services view. In any case, an underlying investigation is generated for you, displaying the Web activity that corresponds to that investigation.

Interpreting the Web activity view

The Web activity view arranges the objects that participate in a web request in six columns. The five first columns are the same columns of the Network activity view: device, user, binary, port and destination. The Web activity view adds a new column: domain. The domain column exposes the visited web domains and

relates them to internal or external destinations. As in the Network activity view, straight lines link the objects of contiguous columns. The lines represent the kind of information selected in the **Display** choice list, found in the top left corner of the diagram, and their thickness is an indication of the amount of data displayed. You can choose to display ingoing or outgoing web traffic, successful or failed HTTP or TLS connections and their duration and response times.

Grouping domains

The objects in the columns of the Web activity view can be collapsed into groups or expanded exactly in the same way as the objects in the Network activity view. In addition, there are some special groups of domains that are created when collapsing individual domains and that you can see when you hover the mouse cursor over the icon of the domain group:

Aliases

Groups domains whose name is not a fully qualified domain name. Aliases usually appear when end-users configure automatic search for local domains. For example, the domain *svn* can be an alias for *svn.intranet.example.com*.

Unnamed

Groups domains that do not have a name. Individual unnamed domains are represented by their IP address.

Named

Fully qualified domain names are grouped by their top-level domain name (com, org, country code, etc).

If there are many domains and they do not fit in their column, you can reach all domains by scrolling with the arrows that appear above and below the column, exactly as you would do with any other column that is also in the Network activity view.

Navigating through paths and objects

The navigation in the Web activity view follows the same rules as in the Network activity view. You can select paths or objects and drill-down or execute one-click investigations in the same way as in the Network activity view. The difference is that the Web activity view does not show information about connections in general, but only about web requests. On the other hand, you have additional information about domains.

When you click on a line of the Web activity joining two objects, a full path from device to destination is highlighted based on your selection. Right-click the path

to drill-down to related objects or activities or execute a related one-click investigation, as you would do from the list results of an executed investigation. You can select several paths at the same time by pressing the **Ctrl** key while you click the paths.

If the Web activity corresponds to an investigation based on objects and not directly based on web requests, a list of objects from the results of the investigation appears to the left of the diagram. For instance, if you execute an investigation on devices and then select the Web activity view, the left hand side of the diagram displays a list of the devices included in the results of the investigation. The list of objects interacts with the displayed lines of the Web activity diagram. If you select a path in the Web activity diagram, the objects that took part in the selected connections are highlighted in the list. The reverse is also true: if you select a specific object from the list, paths representing connections in which the object took part are highlighted in the Web activity diagram. Again, you can select several paths or several objects at the same time by pressing the **Ctrl** key while clicking the lines or the names of the objects. Right-click the name of an object to get the usual drill-down and one-click investigation options associated to the object.

The bar chart of time limited investigations

The functionality of the bar chart in the Web activity view is also very similar to that of the bar chart in the Network activity view. Thanks to the bar chart, you can see a timeline of the web activity and establish the correspondence between bars of activity and paths in the diagram.

If the Web activity view relates to an investigation limited in time (full period investigations and investigations specifying **Between** hours are excluded), a bar chart spanning the period of the investigation appears below the diagram of columns. The height of a bar represents a quantity that depends on the type of information selected in the **Display** choice list, in the same way as the thickness of a line in the diagram does. The value of a bar is valid within the time that corresponds to its width. Hover the mouse over a bar to display the numeric value represented and the time interval that the bar spans. The Finder automatically computes the width of the bars and scales them to fit the time frame of the underlying investigation:

- For a maximum time frame of 7 days, a bar represents 2 hours of data.
- For a minimum time frame of 30 minutes, a bar represents 30 seconds of data.

The bars in the chart also interact with the path lines of the Web activity diagram. Click a bar and the associated paths will be highlighted in the diagram. Click a line of the Web activity diagram and the corresponding sections of the bars will be highlighted in the bar chart. Once again, you can select several lines or several bars by clicking them while you press the **Ctrl** key. Right-click a bar or a group of selected bars to drill-down to related objects or activities or to execute one-click investigations.

Zooming in and out

Limit the number of web requests displayed in the diagram to those that you select using the zoom tool. You can equally limit them to the selected bars in the bar chart.

To limit the number of lines in a diagram to those that correspond to one or more bars in the bar chart, use the **zoom in** icon (the magnifying glass with a plus sign) placed on the top right corner of the Network activity diagram. Selecting one or more bars in the bar chart enables the **zoom in** icon. Click the **zoom in** icon and only the lines that relate to the bars selected will remain displayed in the diagram. After zooming in, come back to the original time frame by clicking the **zoom out** icon that lies to the right of the **zoom in** icon.

In a similar way, you can reduce the number of paths in a diagram to those selected using the zoom. Select one or more paths in the diagram and click the **zoom in** icon. Only the selected paths and their related objects remain displayed in the diagram. Click the **zoom out** icon to come back to the previous zoom level.

Limits of the diagram

The diagram is not able to show more than ten thousand paths. When the maximum number of paths is exceeded, a yellow warning icon shows up in the top right corner of the diagram to inform you that only partial results are displayed.

Viewing executions

To visualize program executions in a graphical way, use the *Local activity* view. The Local activity view relates all the objects that take part in the execution of a program.

To open the Local activity view:

1. Execute an investigation based on executions or on any object that takes part in the execution of a program: device, user, application, executable or binary.
2. From the list of results, click the **Local activity** button placed at the top of the list.

You can also open the Local activity view from other contexts such as the executions section of the device view. In any case, the Local activity view is a graphical representation of an underlying investigation. When you open the Local activity view from a context other than an investigation, the Finder automatically creates the investigation for you.

Interpreting the Local activity view

The Local activity view arranges objects in three columns, one per class of object that participates in an execution: device, user and binary. The Local activity view considers applications and executables as objects that hold binaries. They can appear in the same column as binaries when these are visually collapsed into groups.

The lines that join the object in the columns can represent the number of executions or the duration of the executions in which the connected objects took part, depending on the type of information that you selected in the **Display** choice list in the top left corner of the diagram. The thicker the line that links the objects, the higher the number of executions or the longer the duration of the executions that it represents. You can also make the lines display information about network traffic aggregated during an execution using the **Display** choice list. For detailed information on individual connections, use the Network activity view that is documented in the chapter on Viewing network connections. Alternatively, use the Web activity view, documented in the chapter on Viewing web requests, if you are interested in details about web traffic.

Hovering the mouse cursor over a line in the diagram gives you the exact quantity of the kind of data that the line represents, that is, the kind that you selected in the **Display** choice list. A dashed line indicates zero data.

Grouping objects in the columns of the diagram

The Local activity view shares with the Network activity and the Web activity views the same mechanism for collapsing and expanding objects in the column diagram. When a column contains many objects, the Finder collapses them into groups. You distinguish collapsed objects from single objects by the small plus sign that shows on the icon of the collapsed objects. To expand a group of

collapsed objects, click the plus sign. If a dotted line appears between expanded objects, that means that they share common traits and they are suitable for collapsing. Click the dotted line and the objects linked by the line will collapse. Alternatively, right-click on an object and select **Collapse** or **Expand**. The right-clicking option allows you to force a collapse of objects even when no dotted line links them. As a special case, binary objects can collapse into executables and applications and be displayed as such in the column dedicated to binaries. A collapsed group of devices that displays an additional star on the icon denotes that all members of the group belong to a single entity, which is a special kind of category.

If the number of objects in a column exceeds the vertical space available to show them, an arrow above the column and an arrow below the column help you reach the objects that lie out of bounds. Hover the mouse cursor over the arrows to navigate up or down the objects in the column or click the arrows to navigate quickly.

Navigating through paths and objects

When you click on a line of the Local activity diagram, a full path from device to binary is highlighted based on your selection. Right-click the path to drill-down to related objects or activities or execute a related one-click investigation, as you would do from the list results of an executed investigation. You can select several paths at the same time by pressing the **Ctrl** key while you click the paths.

If the Local activity corresponds to an investigation based on objects and not directly based on executions, a list of objects from the results of the investigation appears to the left of the diagram. For instance, if you execute an investigation on devices and then select the Local activity view, the left hand side of the diagram displays a list of the devices included in the results of the investigation. The list of objects interacts with the displayed lines of the Local activity. If you select a path in the Local activity diagram, the objects that took part in the selected executions are highlighted in the list. The reverse is also true: if you select a specific object from the list, paths representing executions in which the object took part are highlighted in the Local activity diagram. Again, you can select several paths or several objects at the same time by pressing the **Ctrl** key while clicking the lines or the names of the objects. Right-click the name of an object to get the usual drill-down and one-click investigation options associated to the object.

The bar chart of time limited investigations

If the Local activity view relates to an investigation limited in time (full period investigations and investigations specifying **Between** hours are excluded), a bar chart spanning the period of the investigation appears below the diagram of columns. The height of a bar represents a quantity that depends on the type of information selected in the **Display** choice list, in the same way as the thickness of a line in the diagram does. The value of a bar is valid within the time that corresponds to its width. Hover the mouse over a bar to display the numeric value represented and the time interval that the bar spans. The Finder automatically computes the width of the bars and scales them to fit the time frame of the underlying investigation:

- For a maximum time frame of 7 days, a bar represents 2 hours of data.
- For a minimum time frame of 30 minutes, a bar represents 30 seconds of data.

The bars in the chart also interact with the path lines of the Local activity diagram. Click a bar and the associated paths will be highlighted in the diagram. Click a line of the Local activity diagram and the corresponding sections of the bars will be highlighted in the bar chart. Once again, you can select several lines or several bars by clicking them while you press the **Ctrl** key. Right-click a bar or a group of selected bars to drill-down to related objects or activities or to execute one-click investigations.

Zooming in and out

To limit the number of lines in a diagram to those that correspond to one or more bars in the bar chart, use the **zoom in** icon (the magnifying glass with a plus sign) placed on the top right corner of the Network activity diagram. Selecting one or more bars in the bar chart enables the **zoom in** icon. Click the **zoom in** icon and only the lines that relate to the bars selected will remain displayed in the diagram. After zooming in, come back to the original time frame by clicking the **zoom out** icon that lies to the right of the **zoom in** icon.

In a similar way, you can reduce the number of paths in a diagram to those selected using the zoom. Select one or more paths in the diagram and click the **zoom in** icon. Only the selected paths and their related objects remain displayed in the diagram. Click the **zoom out** icon to come back to the previous zoom level.

Limits of the diagram

If the underlying investigation involves a big amount of executions, the Local activity view may not be able to display all the corresponding paths. When the limit of ten thousand paths is exceeded, a warning icon appears in the top right corner of the diagram, to the left of the zoom icons, meaning that only partial results are shown in the diagram.

To see the Local activity diagram in full screen mode, click the growing square icon that is placed to the right of the zoom icons. This is specially useful in diagrams with lots of executions, to help you better distinguish the different paths. To come back to the original view of the diagram, click the shrinking square icon that replaces the growing square icon in full screen mode.

Related references

- [Incoming traffic measurement](#)

Monitoring IT custom metrics

Creating a metric

Overview

Use metrics to measure and survey over time the characteristics of those elements in your IT infrastructure that interest you the most. Metrics reduce complex queries to a single figure, table, or chart that lets you quickly evaluate the state of key components in your IT ecosystem.

To create metrics in the Finder, you must be a user with granted access to the Finder and have the right to edit system content: categories, services, alerts, and metrics.

Creating a metric in the Finder

To create a new metric in the Finder:

1. Log in to the Finder as a user with the appropriate permissions.
2. Select the **Metrics** section from the accordion on the left-hand side of the main window.
3. Right-click the header of the **Metrics** section or the empty area below it.
4. Select **Create new metric** from the menu.
5. Complete the form to define the metric:
 1. Type in the name of the metric.
 2. Optional: Give a short description on the function of the metric.
 3. Fill in each section of the form as described below.
6. Click **Save** to store permanently the definition of the metric.

Retrieve section

Specify the kind of objects used to compute the metric In the **Retrieve** section:

1. In the upper-right part of the section, tick the boxes of the platforms to which the metric applies: Windows, Mac OS or Mobile.
2. Select the type of the objects on which to base the computation of the metric: users, devices, applications, etc.

The choice of a particular kind of object has a logical impact on the grouping options and aggregated values that you can use to define the metric.

Compute daily section

The Portal computes the value of each metric once every day, hence the name of the section. For longer periods of time, the Portal combines the values obtained for a metric over several days in the way that you specify.

In the **Compute daily** section, choose the type of metric that you want to create. Depending on the type of metric, specify how to compute aggregated values for the metric or how to group the retrieved objects when seeing the details of the metric in the Portal.

1. Choose the type of metric from the following options. The word *objects* is replaced by the kind of objects that you selected in the **Retrieve** section:
 - ◆ Count metric
 1. Select **the total number of *objects*** to create a metric that counts objects.
 - ◆ Quantity metric (only available for *device* objects)
 1. Select **the *aggregate of devices*** to create a metric that computes a single value by combining the values of the chosen aggregate in the retrieved devices.
 2. Choose the particular device activity on which to base the metric from the list.
 - ◆ Top metric
 1. Select **the top *N objects with highest / lowest aggregate*** to create a metric that keeps a top list of objects with the highest or lowest value of the specified aggregate.
 2. Choose between 10 to 100 (in increments of 10) the number *N* of objects to display in the top list.
 3. Set either *highest* or *lowest* to order the top list of objects by descending or ascending value of the aggregate respectively.
 4. Select the particular aggregate on which to base the top list.
2. Select the grouping options or aggregate computation when applicable:
 - ◆ For count and quantity metrics, optionally select how the Portal groups the results when you observe the details of the metric. In the **Group by** list:
 - ◇ Select - **none** - if you do not need to group the results.
 - ◇ Select a field or a category to group objects by the value of that particular field or category.

- Optional: Add another field or category after the keyword **and** to define a second criterium to *group by* the objects.
- ◆ For quantity and top metrics, select how to compute the aggregated values for the metric in **Aggregated by**.
 - ◇ For quantity metrics, describe how to combine the individual values associated to each one of the retrieved devices. The Portal applies the selected aggregation method to compute the metric for groups of devices (such as those that share a same location in the hierarchy) and for time frames that span longer than one day. Depending on the aggregate (only the options that make sense for the particular aggregate are available), choose among:
 - **sum over all devices and the whole timeframe**
 - **maximum value per device per day**
 - **average value per device per day**
 - **minimum value per device per day**
 - ◇ For top metrics, describe how the aggregate is computed individually for each object in the top list for periods of time longer than one day. Depending on the aggregate (only the options that make sense for the particular aggregate are available), choose among:
 - **sum over the whole timeframe**
 - **maximum value per day**
 - **average value per day**
 - **minimum value per day**

Matching section

In the **Matching** section, specify a set the conditions that the objects in the **Retrieve** section must meet for taking part in the computation of the metric and, optionally, the hours of the day when the retrieved objects must match those conditions.

The procedure to define these conditions in the **Conditions** part of the definition of a metric is very similar to setting the conditions of an investigation. Conditions are a set of rules that apply to any item (object, activity or event) that is related to the objects selected in the **Retrieve section**:

To add a new condition:

1. In the **Conditions** subsection, click the link **Click here to add a new condition**. The placeholders for the condition fields show up.

2. Set the object, activity, or event to which the condition applies.
3. Set the attribute or category that you want to constraint.
4. Set the operator for comparison (e.g. *is*, *is not*, *starts with*, etc).
5. Set the matching value, if you selected an attribute constraint, or the matching keyword, if you selected a category constraint.

Some combinations of conditions and display settings are incompatible. If you add a condition and a red exclamation mark appears on its right side, the condition may conflict with another condition or with one of the chosen attributes to display. Hovering the mouse over the exclamation icon will tell you the reason for the conflict

To delete a condition:

1. Click the trash icon to the right of the condition fields.

For count metrics, an additional setting specifies how objects are counted when the time frame in the Portal is longer than one day:

1. Choose either **at least one day** or **the last active day** from:
Count objects that meet conditions on *at least one day / the last active day* in period

As a guideline, select **at least one day** when you want the metric to account for event occurrences during the period. For instance, a metric that counts the number of devices with hard resets. For a device to be counted, the hard reset can happen any time during the interval. On the other hand, select **the last active day** for metrics that have an inventory function. For example, a metric that counts the number of devices with two monitors. Indeed, if a device does not have two monitors on the last day of the period, it must not be added to the inventory.

Optionally, restrict the time of the day to which the computation of the metric applies by ticking the check box and setting the start time and the end time of the computation in the last line of the **Matching** section:

- **Between *HH:MM* and *HH:MM*.**

Options section

The contents of the **Options** section depend on the type of metric that you selected.

For count metrics, the following options are available:

1. Tick **Include ratio** to get a percentage in addition to a cardinal number as the displayed value of the count metric in the Portal.
 - ◆ The percentage is computed as the number of objects that match the conditions defined in the metric divided by the number of objects that match another set of conditions.
 - ◆ Define the new set of conditions in the same way as you defined the conditions for the metric with the tools that show up when you tick the **Include ratio** check box.
2. Tick **Include variation and threshold indicator** for the Portal to display changes in the value of the metric with respect to its last value and indicate whether a value increase or decrease is a positive or a negative thing for you. Select one from these three options:
 - ◆ **variation indicator only**
 1. By default, a green arrow up and a red arrow down are displayed below the statement, meaning that an increase in the value of the metric is a positive thing. For instance, an increase in the number of devices with antivirus is a good thing.
 2. To change the default and indicate that a value increase of the metric is a negative thing, click **invert** to switch the two arrows. For example, an increase in the number of bluescreens is a bad thing.
 - ◆ **variation indicator and 1 threshold**
 1. Choose the direction of the variation indicator by clicking **invert** if appropriate (see first option).
 2. Set the value of the threshold on top of the horizontal arrow. Only when the increase in the value of the metric is higher than the threshold, the indicator changes color (to green if increase is good, to red if it is bad).
 3. If you ticked the option **Include ratio**, you may want to define the threshold as a ratio:
 1. To the right of the variation message, choose between **absolute** or **ratio** values (Include *variation message* based on *absolute / ratio* values).
 - Choose **absolute** to express the threshold in number of objects, as in the case described above.
 - Choose **ratio** to express the threshold in a percentage related to the ratio value computed for the metric.

- ◆ If you choose *ratio* you can ignore the threshold value when grouping results by hierarchy in the Portal if the number of devices in a node of the hierarchy is too small. Tick the option **Ignore threshold if there are less than N devices in a hierarchy node** and set a value for N .

- ◆ **variation indicator and 2 thresholds**

1. Choose the direction of the variation indicator by clicking **invert** if appropriate (see first option).
2. Set the thresholds in the same way as explained in the 1 threshold case. You can also express the thresholds in percentage values if you ticked the **Include ratio** option. The only difference with the 1 threshold option is the addition of the yellow color:
 - If the increase in value of the metric is higher than the first threshold, the variation indicator turns yellow.
 - Only when the increase in the value of the metric is higher than the second threshold, the variation indicator changes color (to green if increase is good, to red if it is bad).
3. Set the **Additional display fields** as in the display section of an investigation.
 1. Check all the fields of the objects retrieved by the metric whose data you are interested in.
 2. Later, select in the Portal which one of these fields to display when you see the details of the metric.

For quantity metrics, only the options for the variation indicator and thresholds are available. Refer to step 2 of count metrics for instructions. Ignore the suboptions related to ratio, since these are not supported by quantity metrics.

In the case of top metrics, only the option to set additional display fields is available. Refer to step 3 of count metrics for instructions.

Related concepts

- Metric

Examples of metrics

Overview

Creating a new metric may be a daunting task for beginners because of the many options available. To help you with the creation of metrics, let us walk through an example that covers the creation of three metrics, each one of a different type: count, quantity, and top.

The example gets information on binaries that are considered dangerous. To that end, we propose the creation of three metrics, which the reader can later refine and expand:

Devices executing dangerous binaries

Count the number of devices that execute dangerous binaries.

Cumulated execution time of dangerous binaries

Measure how long your devices were exposed to the execution of dangerous binaries.

Top most executed dangerous executables

List the top ten executables associated to dangerous binaries by number of executions.

In this example, we consider a binary to be dangerous when its **Threat level** field is set to *high threat*. Nexthink automatically sets the value of this field via the application library. You may later come up with your own definition of a *dangerous* binary and adapt the conditions in the example metrics accordingly.

For every step in the creation of the metrics that requires the choice of an option, we explain our decision in detail. We assume however that you know the basics of creating a metric.

Count metric

The first metric reflects the number of devices impacted by the execution of dangerous binaries.

Create a count metric in the Finder and edit its options:

1. Type in the name of the metric: **Devices executing dangerous binaries**.
2. Optional: Type in a description for the metric.
3. In the **RETRIEVE** section, click **devices**.
4. In the **COMPUTE DAILY** section:

1. Select the option **the total number of devices** to create a *count* metric.
2. Assuming that we might be interested in the status of the antivirus of those devices executing dangerous binaries, choose **Group by *antivirus up-to-date* and *antivirus RTP*** to classify the devices by the update status of their antivirus and their activation of the real-time protection.
5. In the **MATCHING** section:
 1. Add the condition **Binary Threat level is high**.
 2. Leave the default option **Count devices that meet conditions on *at least one day* in period**. We want to count the devices that executed a dangerous binary anytime within the observed interval (that is, the period that you set in the navigation tool of the Portal when watching the results of the metric). We do not select thus the option *the last active day*, which is intended for metrics that have an inventory function.
6. In the **OPTIONS** section:
 1. Tick the box **Include ratio** without including any new condition. In that way, you compare the number of impacted devices with the total number of devices.
 2. Tick the box and select the option **Include *variation indicator only***. We do not need to set any threshold and we keep the default option for the sense of the variation: an increase in the value of the metric is bad (red arrow up) and a decrease of its value is good (green arrow down).
 3. Optional: Tick any of the **Additional display fields** that you want to add.

Quantity metric

As second metric, let us measure for how long dangerous binaries have been executing on the devices.

Create a new metric and edit its options:

1. Type in the name of the metric: **Cumulated execution of dangerous binaries**.
2. Optional: Type in a description for the metric.
3. In the **RETRIEVE** section, click **devices**, since quantity metrics can only be selected for devices.
4. In the **COMPUTE DAILY** section:
 1. Select the second option to create a *quantity* metric and build the sentence: **the *cumulated execution duration of devices***.

2. In the group by option, keep the default - **none** -, as we do not need to break down the results.
3. In the aggregate by option, select **sum over all devices and the whole timeframe**. We are interested in the total execution time over all devices and not in the average execution time per device, which is the other available option.
5. In the **MATCHING** section:
 1. Add the condition **Binary Threat level is high**.
6. In the **OPTIONS** section:
 1. Tick the box and select the option **Include variation indicator and two thresholds**. We want to set warning and error conditions if the cumulated execution time of dangerous binaries exceeds some values.
 2. In the bar to indicate the thresholds, keep the sense of variation (red arrow up, green arrow down) and set the first threshold to **10 min** and the second to **1 hours**.

Top metric

Finally, let us add a metric that retrieves the top 10 most executed executables whose binary representations are considered dangerous. Remember that an executable in Nexthink groups the different versions (binary images) of a program in a single object. In this case, a metric retrieving executables is probably more convenient than a top metric retrieving the individual binaries. Indeed, having a list of different executables is preferable to seeing different binary versions of the same executable repeated in a list.

Create a new metric and edit its options:

1. Type in the name of the metric: **Top most executed dangerous executables**.
2. Optional: Type in a description for the metric.
3. In the **RETRIEVE** section, click **executables**.
4. In the **COMPUTE DAILY** section:
 1. Select the second option to create a *top* metric and build the sentence: **the top 10 executables with highest number of executions**.
 2. In the aggregate by option, select **maximum value per day**. A perfectly valid option as well would be **sum over the whole timeframe** to see the total number of executions of each executable. For this time, however, we want to classify the executables by their maximum burst of executions in one day and, in that way, find out the dangerous executables which are run more

aggressively. We are not much interested either in the other available aggregation option **average value per day**, because we want to detect the extreme cases.

5. In the **MATCHING** section:

1. Add the condition **Binary Threat level is high**.

6. In the **OPTIONS** section:

1. Optional: Tick any of the **Additional display fields** that you want to add.

Conclusion

We hope that this example has helped you clarify some of the concepts behind the creation of a metric. Keep on reading to know how to create widgets in the Portal to display the values of the metrics in the Portal. For more information on how the Portal computes and presents metric data, read this article on aggregation and grouping.

Related tasks

- Creating a metric

Related references

- Portal aggregation and grouping
- Nextthink Application Library

Following the evolution of a metric

Overview

After defining a metric in the Finder, follow the evolution of its value from the Portal. Choose among different visualizations (*widgets*) for your metric.

To add metrics to the Portal, you must be a user with the right to create personal dashboards. If you do not have the right to create your own dashboards, you can still see the dashboards attributed to your roles.

Adding a metric to the Portal

To add a metric to the Portal, insert it into a dashboard. You may either reuse an existing dashboard or create a new one. In any case, the dashboard must belong

to a module of type *blank*.

Dashboards in blank modules are initially empty, displaying just a blank page where you can add and organize widgets for your metrics, hence their name. Combine several types of widgets in a dashboard to see your metrics from different points of view.

To create a new blank module and dashboard:

1. Click the menu icon (three bars) on the right-hand side of the dark blue ribbon.
2. Select **Create new module...** at the bottom of the menu.
3. Choose **Blank module** as the type of module to create.
4. A new blank module with a default empty dashboard appear in your Portal.
5. Optional: Rename the module and the dashboard (by default **Untitled module** and **Untitled dashboard**) by clicking the menu icon again and selecting **Rename....**
 1. Type in the new names for both the module and the dashboard under **Module name** and **Dashboard Name**.
 2. Click **Done**.

Alternatively, choose an existing dashboard from the module navigation tool that you find on the left-hand side of the dark blue ribbon:

1. Click the module navigation tool (it displays the names of the current module and dashboard).
 - ◆ If you have the permissions to see published content, and there actually are some modules published, you may see the rubrics **My content** and **All published**.
 1. Click **My content** if this is the case.
2. Select a blank module from the section **PERSONAL**. Only those modules that belong to you are available for editing.
 - ◆ If you do not see the section **PERSONAL**, you do not have permissions to create dashboards. Ask your administrator.
 - ◆ If the **PERSONAL** section is empty of modules, it displays the message **No personal module. Click here to create one.**
 - ◇ Click the word **here** in the message to create your first personal module as an alternative to the method seen above.
 - ◇ Select a dashboard from any of the other sections (dashboards included in your roles or under the **All published** rubric, if available) and copy it to your personal

section to be able to modify it:

1. Click the menu icon on the right-hand side of the blue ribbon once the dashboard is open.
2. Select **Copy module to my content** from the menu.
3. Select one of the available dashboards in the module.

Once you have either the new or the existing dashboard in your screen, add the metric to it:

1. Click the menu icon on the right-hand side of the dark blue ribbon.
2. Select **Edit content** in the **DASHBOARD** section. The dashboard is now in edition mode.
 - ◆ If the dashboard was empty, a plus sign appears on it.
 - ◆ If the dashboard has content, plus signs appear while you hover the mouse over the limits of existing widgets.
3. Click one of the plus signs to add a new widget for your metric at that location of the dashboard.
 - ◆ Note that widgets can hold more than one metric. If you prefer to add your metric to an existing widget, click the sprocket icon that appears when you hover the mouse over the top-right corner of a widget and select **Edit**.
4. Choose the type of widget that you want to create:
 - ◆ KPI
 - ◆ Table
 - ◆ Line Chart
5. Fill-in the dialog to add the widget:
 1. Optional: Type in a title for the widget.
 2. Click the button **Add metrics**.
 3. Select a metric from the list of available metrics.
 4. Click the button **Add**. The list of metrics turns into a preview of the widget.
 5. Depending on the type of widget that you chose, set the **DISPLAY** options.
 6. Optional: Click **Add metrics** again to add as many metrics as you want to the widget.
 7. Click **Done** to finish editing the widget and come back to dashboard edition.
6. To finish editing the dashboard, click the check mark that replaces the menu icon on the right-hand side of the dark blue ribbon while in edition mode.

Related references

- Types of widgets

Monitoring IT services

Analyzing service quality

Overview

Today, companies strongly depend on a set of IT Services to carry out their daily work. Although the particular set of deployed IT services may vary from one company to another, the correct functioning of services is vital for the day-to-day business of every organization.

With Nexthink, define the IT services that you want to survey by specifying their characteristic resources and see how well those IT services perform inside your corporate network. Thanks to the user-centered approach of Nexthink, you get a glimpse on the quality of the service as it is perceived by the end-users. See in real-time the status of a service and find out who are the impacted users when the service degrades. In the case of service degradation, Nexthink may help you determine where the problem lies. For long term analysis, follow the evolution of the service throughout extended time intervals.

Nexthink divides IT services into two types:

Connection-based services

Services that rely on TCP connections for providing their solutions to the users. Both Windows and Mac devices report information on connection-based services.

Applies to platforms:

Web-based services

Web sites or web applications that use the HTTP protocol or its encrypted variant with TLS (HTTPS) to provide a service to their users. Web-based services also rely on TCP for transport, but defining the service at the HTTP level lets you filter the service by the accessed web domains or URLs. For the moment, only Windows devices report information specific to web-based services.

Applies to platforms:

Service metrics

The type of service determines the exact metrics that are used to measure its performance. The set of metrics is nevertheless very similar for both connection-based and web-based services. Most of the metrics are shared or serve a similar purpose in both types of services. See below a list of all the metrics where the shared metrics are emphasized:

Connection-based service metrics	Web-based service metrics
<ul style="list-style-type: none">• <i>Devices with issues</i>• <i>Devices using service</i>• Failed connections• <i>Application crashes</i>• <i>Average response time</i>• Incoming traffic• Outgoing traffic• Incoming bitrate• Outgoing bitrate	<ul style="list-style-type: none">• <i>Devices with issues</i>• <i>Devices using service</i>• Failed web requests• <i>Application crashes</i>• <i>Average response time</i>• Incoming web traffic• Outgoing web traffic

Analyzing services in the Finder and the Portal

To analyze service quality, Nexthink offers you two possibilities:

The Service View in the Finder

The Service View provides you with a real-time view of the service, including the values of the service metrics for the last 60 minutes and the last 24 hours. Break-down results according to entities in your hierarchies, drill-down to individual connections or devices, and quickly switch to the Network or Web views directly from the Service View.

The service dashboards in the Portal

Service modules summarize the status of your services in a special overview dashboard. Moreover, for each individual service in the module, a detailed service dashboard provides you with a full view of the service key metrics through a comprehensive set of widgets. In addition to a real-time view for the last 60 minutes and the last 24 hours, the Portal lets you select longer periods of time to see historical values and trends in your service-related data.

Related tasks

- Creating a service
- Observing service performance

- Following the evolution of a service

Related concepts

- Service

Related references

- Real-time and consolidated service data

Creating a service

Overview

Define services in the Finder, based either on web connections or on lower-level TCP connections, by specifying one or more of the following:

- The destinations (servers) that provide the service.
- The web domains that host the service (only for web-based services).
- The executable files of the applications that access the service.
- The ports that applications use to connect to the service.
- The devices that consume the service (useful for limiting the devices monitored rather than for defining the service).

Nexthink automatically associates the network connections that match the given specifications to the service thus defined, helping you keep track of the status and utilization of your IT services.

In addition, to survey the health status of services more easily, set thresholds on the number of devices with issues that access a service. Color codes -green, yellow, and red- help you distinguish whether the service is doing fine or not, depending on whether the thresholds are respected or exceeded.

Procedure

To create a new service in the Finder:

1. Select the **Services** section from the accordion on the left-hand side of the main window.
2. Right-click the header of the **Services** section or the empty area below it.

3. Select **Create new service** from the menu. The Finder displays the form to define the service.
4. Give a name to the service.
5. Optional: Give a short description of the service.
6. Select the type of service:
 - ◆ Check **Network connections** to create a connection-based service.
 - ◆ Check **HTTP and TLS web requests** to create a web-based service.
 - ◆ Check **HTTP web requests with URL path** to create a web-based service by specifying a URL path. Remember to configure the Collector to send path information.
7. Specify the devices that connect to the service.
 - ◆ **any**: Record the connections from any device to the service.
 - ◆ **with name**: Record only the connections to the service of the device with the given name.
 1. Type in the name of the device. You can use the substitution characters * and ? as indicated in the tooltip.
 - ◆ **with IP network**: Record only the connections of the devices with at least one of their IP addresses belonging to the given subnetwork.
 - ◆ **with keyword**: Record only the connections of the devices tagged with the given keyword.
 1. Select a category of devices from the list.
 2. Select a keyword of the chosen category from the list.
8. Specify the executables that connect to the service.
 - ◆ **any**: No matter what executable can establish a connection to the service.
 - ◆ **with name**: Only the executable with the given name connects to the service.
 1. Type in the name of the executable. You can use the substitution characters * and ? as indicated in the tooltip.
 - ◆ **with keyword**: Only the executables tagged with the given keyword connect to the service.
 1. Select a category of executables from the list.
 2. Select a keyword of the chosen category from the list.
9. Specify the TCP ports reserved for the service.
 - ◆ **any**: No particular TCP port is reserved to connect to the service.
 - ◆ **with number**: The service is bound to the TCP port with the given number.
 1. Type in the port number.
 - ◆ **with keyword**: Only the TCP ports tagged with the given keyword are characteristic of the service.

1. Select a category of ports from the list.
 2. Select a keyword of the chosen category from the list.
10. Specify the destinations that provide the service.
- ◆ **any**: The destination of the connection is not relevant for defining the service.
 - ◆ **with IP address**: Only the connections to the destination with the given IP address are associated to the service.
 1. Type in the IP address of the destination (e.g. 192.168.3.1).
 - ◆ **with IP network**: The service is offered by a group of destinations belonging to the given subnet.
 1. Type in the IP subnetwork in CIDR notation (e.g. 192.168.3.0/24).
 - ◆ **external**: The service is offered by destinations outside the monitored networks.
 - ◆ **with keyword**: Only the destinations tagged with the given keyword offer the service.
 1. Select a category of destinations from the list.
 2. Select a keyword of the chosen category from the list.
11. When creating a web-based service, specify the domains that belong to the service:
- ◆ **any**: The service is not restricted to any domain in particular. This option is not available if you are creating a web-based service with URL path.
 - ◆ **with name**: Only the domain with the specified name belongs to the service.
 1. Type in the name of the domain. You can use the substitution characters * and ? as indicated in the tooltip.
 - ◆ **with keyword**: Only the domains tagged with the given keyword belong to the service.
 1. Select a category of domains from the list.
 2. Select a keyword of the chosen category from the list.
 - ◆ Additionally, if you are creating a service with URL path:
 1. Type in the **URL Path** that the service will recognize as its own.
12. Recommended: Tick the box **Set threshold on devices with issues** to specify the minimum quantity of impacted devices needed for considering that the service is degraded or down. The message changes to **Set 1 threshold / 2 thresholds on devices with issues, considering errors only / errors and entity warnings**.
- ◆ Select **1 threshold** to define two statuses for the service: ok (green), or error (red).

In the colored bar below the message, set the required percentage of devices that must have issues for the service

to turn its status from ok to error.

- ◆ Select **2 thresholds** to define three statuses for the service: ok (green), warning (yellow), or error (red).
In the colored bar below the message, set the required two percentages of devices with issues for the service to turn its status from ok to warning, and from warning to error, respectively.
 - ◆ Select **errors only** to count as devices with issues only those devices in the error state.
 - ◆ Select **errors and entity warnings** to also count in those devices that belong to entities in the warning state, in addition to devices with errors or in an entity in the error state (see Service errors and warnings).
 - 1. Optional: Tick the box **Ignore unless at least *N* devices are impacted in a hierarchy node** to take into account the percentages indicated as thresholds only if *N* or more devices within a node of the hierarchy have issues. This is useful to avoid false alarms (services in error state) in nodes with few devices.
13. Click on **Save** to store your new service permanently.

Follow the evolution of services either from the service view of the Finder or from the Portal. Setting thresholds helps you quickly distinguish those services that are working as expected from those which may require intervention.

Limit on the number of services

Using this procedure, define as many services as you wish. However, for performance reasons, a maximum of **100 services** may be simultaneously enabled. If you have defined more than 100 services, those in excess are disabled; meaning that they do not receive any connection nor, in consequence, display any data..

Related tasks

- Following the evolution of a service
- Specifying URL paths of web-based services

Related references

- Service errors and warnings

Related concepts

- Service
- Device
- Executable
- Port
- Destination
- Category
- Keyword

Following the evolution of a service

Overview

In Observing service performance you have learned how to interpret the service view in the Finder. The Portal offers you a different perspective on services, allowing you to see not only real-time data, but also longer time intervals for historical data and trend analysis.

Adding a service dashboard to the Portal

To add a service to the Portal, create a dashboard for it. You can either add the dashboard to an existing service module or create a new service module. Only modules of type *service* can hold service-based dashboards.

To create a new service module:

1. Log in to the Portal as administrator or as a user with the right to create personal dashboards.
2. Click the menu (three bars) icon on the right-hand side of the dark blue ribbon.
3. Select the last option **Create new module...**
4. Select **Service Monitoring** to create a new module for hosting services.

Alternatively, navigate to an existing service module using the navigation tool on the left-hand side of the dark blue ribbon. The tool displays the names of the module and dashboard that are currently active in the Portal:

1. Click the names of the current module and dashboard.
2. Select a service module from the section **My content**, since only those modules that belong to you are available for editing.
3. Open the **Overview** dashboard or any other dashboard of a service in the module.

4. Click the menu icon on the right-hand side of the dark blue ribbon.
5. Select **Configure module....**

Once you have created a new service module or entered the configuration of an existing service module, add the desired service (or services) to it:

1. From the list of available services, select those that you want to see in the module and click the button with the arrow pointing to the right. Services move from the **AVAILABLE** list to the **SELECTED** list.
2. Optional: If you selected some services by mistake, select them again and click the button with the arrow pointing to the left. Services move from the **SELECTED** list back to the **AVAILABLE** list.
3. Optional: All service modules have an **Overview** dashboard where you can see the list of all other dashboards in the module, each one representing a different service. Select how you want to arrange this list of services and their status break down, whether in rows or in columns, by setting the option **In overview dashboard, display services as rows / columns**.
4. To end adding the service (or services), click **Create**, if you are creating a new module, or **Done**, if you are modifying an existing module.

Specifying URL paths of web-based services

If you have purchased the Web and Cloud module, you can define services in Nextthink for measuring the connectivity of the end-users to web applications and web sites by stating the domain name of the particular provider of the service. In some cases though, you may want to differentiate among several services that lie within the same domain. For instance, you may want to make the difference between:

- www.example.com/agenda
- www.example.com/share

To treat these two addresses as different services, you must first configure your Collectors to report the URLs of the web requests addressed to the domain www.example.com.

Then create two services in the Finder of the type **HTTP web requests with URL path**. In addition to the name of the domain, you can specify now a URL path to distinguish services within the same domain. Note however that the URL path option is only available for HTTP and not for TLS web-based services. Following with our example, you would specify as URL paths:

- agenda
- share

All subpaths are naturally included in the definition. You may also use the star pattern to substitute for zero or more characters in the URL path.

Domain	URL path	Matches
www.example.com	agenda	<ul style="list-style-type: none"> • www.example.com/agenda/mycal.php
	share	<ul style="list-style-type: none"> • www.example.com/share/myshare.html • www.example.com/share/groupshare.html
	sh*	<ul style="list-style-type: none"> • www.example.com/share/myshare.html • www.example.com/sharing/index.html

Related tasks

- Creating a Service
- Reporting the URL of HTTP web requests

Organizing objects with categories

Classifying objects of the same type

Overview

Nextthink distinguishes ten types of objects to describe your IT infrastructure:

• User	• Package	• Executable	• Port	• Domain
• Device	• Application	• Binary	• Destination	• Printer

When you create an object-based investigation or widget, you target a particular type of object. Object types are predefined and their number is fixed. However, you might want not to target all the objects of a type, but only a custom-defined subset. To that end, Nextthink introduces the concept of *Categories*. Categories work one level below the object type, defining classes of objects within objects of the same type. For instance, you can create different classes of users, devices or applications according to the processes and policies in your own organization. The ability to define your own subtypes of objects lets you create investigations and widgets specifically targeted to those subtypes.

Each category applies thus to only one type of object. The category defines a set of classes, each one identified by a *keyword*, that partitions the group of all the objects of the given type into disjoint subsets. Therefore, at most one keyword per category can be assigned to an object. If an object does not fit into any of the classes defined by the category, the object gets assigned the *empty* keyword for that category.

Tagging objects

The process of assigning keywords to objects is called *tagging*. A tag is a label consisting of a pair **Category:Keyword** that is attached to the object. Tagging can be manual, automatic (based on a set of auto-tagging rules) or semi-automatic (based on tags loaded manually from a CSV file).

Displaying the tags of objects

For object-based investigations, optionally display a column for each available category. Add the desired category-related columns either when editing the options of the investigation or while navigating through the list of results. The

columns of categories show the keywords assigned to each object.

If a keyword is assigned to an object as a result of automatic tagging, a small icon with the letter *A* appears to the right of the name of the keyword. If you tag the object manually or you import the tag from a file, no special indication is given.

Platforms and automatic tagging of devices

When you automatically tag devices based on the value of one of their attributes, remember that not all attributes are present in devices of different platforms.

Related tasks

- Editing the options of an investigation
- Navigating through the results of an investigation
- Tagging objects manually
- Tagging objects automatically
- Importing tags from text files

Creating categories and keywords

Categories and keywords let you classify objects of the same type into user-defined groups. Only users with the appropriate permissions can create or edit categories.

Create a new category

To create a new category using the Finder:

1. Go to the **Categories** section on the left-hand side of the main window.
 - ◆ If you want to create the new category at the top-level, right-click the header or the empty area of the **Categories** section.
 - ◆ If you want to create the new category inside a particular folder, right-click an existing folder in the **Categories** section.
2. Select **Create new category**.
3. From the choice list, select the type of object on which the new category is based.
4. A new category, with the temporary name **Untitled Category n**, where *n* is a growing number to avoid name clashes, shows up in a new tab.
Optional: Click the name of the category and replace it with an appropriate

- name.
- Optional: Click the field below the name of the category labeled **Enter description here...** and give a short description on how the new category classifies objects.
 - Select the level of privacy associated to the category. For more information, see the chapter on Privacy.
 - Add new keywords to the category (follow the set of instructions below).
 - Optional: Depending on the number of the keywords that you define, creating a category can be a lengthy process. Click the **Save** button after a worthy modification to make sure you do not lose your job.
 - Click the **Save and close button** to save your last changes and close the edition tab. Alternatively, click the **Close** button if you already saved your work.

Edit an existing category

To edit a category:

- Find the category to edit. You can either:
 - ◆ Search the name of the category in the Search box of the welcome screen
 - Click the desired result of the search.
 - ◆ Browse the **Categories** section on the left-hand side of the main window.
 - Right-click the name of the category.
 - Select **Edit...**
- Modify the name, description or keywords of the category.
- Click **Save and close**.

Add and edit keywords

To add new keywords to a category:

- Create a new category or edit an existing category.
- Locate the buttons for editing keywords at the bottom left corner of the panel.
- Click the button with the plus sign to add a new keyword.
- Type a name for the new keyword and click **OK**. You cannot repeat the same name for a keyword in a category.
- Optional: Set the auto-tagging conditions for the keyword. See the chapter on Tagging objects automatically.
- Optional: To save you some work, click the button picturing two documents to make a copy of an existing keyword if you need to create

similar classes of objects. The auto-tagging conditions that you defined for one keyword are copied to the other.

7. Optional: Click the button with a pencil to rename a keyword.
8. Optional: Click the button with the trash can to remove a keyword.

All the functions of the buttons for editing keywords are also available in a context menu by right-clicking the **Keywords** panel.

Related tasks

- Adding users (create a profile that allows the edition of categories)

Tagging objects manually

Once you have defined a category, you can manually tag the objects of the type associated to the category. *Tagging* is applying a keyword of a category to an object. Thus the object becomes a member of the class of objects identified by the keyword.

Some category keywords include auto-tagging conditions in their definition for tagging objects automatically. Other keywords may not define any auto-tagging conditions. To manually tag objects you can use both types of keywords: with or without auto-tagging conditions.

In any case, note that when you tag an object manually, you override the automatic tagging based on conditions for that object. Despite the override, manually tagging an object does not change the definition of a category keyword. The modification applies to the object locally in the Engine and not to the definition of categories, which are themselves centralized and apply to all Engines.

To manually tag an object with a keyword in the Finder:

1. Find the object to tag in the list of results of an investigation. For that purpose, you can use the default investigation that executes after you edit the category that defines the keyword.
2. Right-click the name of the object and select **Edit...** A dialog with the list of all the categories that you can apply to the object pops up.
3. Next to each category, you have a drop down list to choose a keyword for the object. By default, the system tags objects automatically, so the option **auto** appears selected in the drop down. Click the down arrow of the drop down list to see all the available keywords for that category.

4. Select the desired keyword to tag the object. Otherwise, you can assign the *empty* keyword or let the system automatically tag the object by choosing the *auto* option.
 - ◆ Optional: If you do not find a suitable keyword for the object, you can add a new keyword to the category by selecting **Add new keyword...** from the drop down list.
5. If the operation was successful, the dialog finishes with a message displaying the number of objects that were updated. Click **OK** to close the dialog.

You may apply the same keyword to a group of objects if you select several objects instead of just one. Use the **Ctrl** key to click multiple objects or the **Shift** key to select a range of objects in the list. Then right-click and proceed as explained above.

Related references

- Local and shared content

Tagging objects automatically

Depending on the number of objects to classify, tagging objects manually can be a very long and inefficient process. Alternatively, you can let the system automatically tag objects for you, as long as you instruct the system on how to classify objects according to the values of their attributes. This is done by assigning *auto-tagging conditions* to the keywords of a category.

Defining auto-tagging conditions

To define auto-tagging conditions for a keyword in the Finder:

1. Create or edit a category (see the chapter on Creating categories and keywords).
2. In the **Keywords** panel, select the desired keyword. The right hand side of the panel shows the auto-tagging conditions for the keyword. If no condition has been defined yet, this part of the panel is empty the keyword is never assigned automatically to any object.
3. Click the link **Click here to add a new condition** to specify an auto-tagging. The way to express auto-tagging conditions is similar to the way you specify the conditions of an investigation. A row with three drop down lists appears.

4. Choose the attribute of the object whose value will be compared in the first drop down list. For device objects, beware that all attributes are available for selection, but not all of them are necessarily available for all of the platforms.
5. Select a comparison operator in the second drop down list.
6. In the last drop down list or combo box, select or type the value to compare with the selected attribute. Once you define a condition for a keyword, a small icon with the letter *A* appears to the left of the name of the keyword in the panel, indicating that the keyword is used in automatic tagging.
7. Optional: Click the trash can placed to the right of the drop down lists to remove a condition.
8. Optional: Go back to point 3 to add new conditions. If you create more than one auto-tagging condition for one keyword, you can specify how the conditions combine using the **Logical expression** field that appears below the conditions. By default, conditions are combined by a logical or. Therefore, it is enough for an object to fulfil one of the conditions to be tagged with the keyword. You can use the logical operators *OR* and *AND* to combine the auto-tagging conditions of a keyword.
9. Click **Save** to permanently save your work and continue editing the category or **Save and Close** to save your work and end the edition of auto-tagging conditions.

Setting the precedence of automatic keywords

An object can be tagged by at most one keyword per category. If an object satisfies the auto-tagging conditions imposed by two or more different keywords, the system tags it with only one of the keywords. You can decide what keywords take precedence over others by establishing a ranking of automatic keywords. Remember that tagging an object manually overrides any automatic assignment of keywords.

To set the precedence of automatic keywords in the Finder:

1. Create or edit a category that holds automatic keywords, that is, keywords that specify auto-tagging conditions (see above).
2. Click the button **Set auto-tagging order...** located below the list of keywords. A dialog pops up with the list of all the automatic keywords, ordered by precedence. By default, keywords are ordered in alphabetic order.
3. Click the name of a keyword in the dialog to change its order of precedence.

4. Click the button **Move up** to promote the selected keyword to a higher rank or the button **Move down** to lower the precedence of the keyword.
5. Click **OK** once you are satisfied with the ordering of keywords or **Cancel** to ignore the changes made.

Performance considerations

Nextthink triggers the automatic tagging process for all objects of a given type when you create or modify a category that applies to that type. The modification of a category can indeed imply a modification of the auto-tagging conditions, so every object must be rechecked against the new conditions. At a lower scale, the modification of the attributes of an object may also trigger the automatic retagging of the object. If the modified attribute is suitable for comparison in auto-tagging conditions, the new value of the attribute can make the object fall into a different class and, therefore, be tagged with a different keyword.

Although the system does not impose a hard limit on the number of categories and keywords that you can define, automatic tagging can become a costly operation depending on the number of computations required. Specifying too many keywords or auto-tagging conditions may have a significant impact in the overall performance of the system. The maximum recommended values for keeping the system responsive are listed below:

- 25 categories per type of object (device, user, application, etc).
- 200 automatic keywords per category.
- 20 auto-tagging conditions per keyword.

Importing tags from text files

Overview

Importing tags from a file is a semi-automatic way of tagging objects. Tagging with the help of a text file with CSV format is particularly useful in situations where the classification of objects depends on an external source of information. In such cases, you cannot use automatic tagging because the classification is independent of the attributes of the object and using manual tagging can take too long if the number of objects to tag is high.

The result of importing tags from a file is the same as if the objects were tagged manually. That is, importing tags overrides automatic tagging for the objects and the categories involved. As in manual tagging, importing tags from a text file

changes the objects locally in a particular Engine and not the objects in other Engines nor the definition of the categories. Categories are centralized, but importing tags from text files is not.

Again, because tagging from text files is equivalent to manual tagging, the last tag that is applied to an object (within a category) is the tag that prevails. In your CSV file, if multiple tagging rules that belong to the same category match a particular object, the import process successively tags the object for every matching rule. Therefore, the last matching rule in the file gives the object its definitive tag. Beware that the list of rules may appear differently in the import dialog. The order of the rules in the file determines their order of application.

Format of the CSV file

The file to import must be a text file organized as a table, where each line of text represents a row of the table and a delimiter character (usually a comma) separates values into columns within a row. This is commonly known as a *Comma-Separated Value* file or CSV file. For the purpose of importing tags, the CSV file is organized into columns of keywords. The first element of each column is the name of the category to which the keywords in the column belong. A special column is used to match the lines of the CSV file with the objects to be tagged. Unlike other columns, this column does not hold keywords of a category, but values of an attribute that designates the object to be tagged. Only attributes that identify an object, such as the ID or the name, can be used to do the match. The allowed attributes for matching depend on the type of the object. Each line of the CSV file can therefore be seen as a row of a table, where one value identifies the object to be tagged and the rest of the values are the keywords that will be applied to the object.

The CSV file can have other columns with information that is not related to categories. These columns can be ignored during the import process.

Limit on the size of the CSV file

The maximum size of the CSV file to import tags is **140 KB**, which corresponds approximately to 2'500 rows.

If the number of objects to tag is bigger, split the CSV file into two or more files and import them separately.

Import process

To import tags from a CSV file:

1. In the Finder, click the sprocket icon located on the right hand side of the header of the main window.
2. Select **Import tags from file...** from the menu.
3. Choose the CSV file in the standard dialog to open files. A wizard to set the import options shows up.
4. Select the text encoding (e.g. Western European or UTF), the character that delimits columns (e.g. comma or semicolon) and the character that qualifies a value as text (e.g. single or double quotes).
5. Optional: Click the button **Show file** to see the file that you are importing. This is useful to validate your previous selection of text encoding and special characters.
6. Click **Next** to go on with the import process.
7. Select the type of the objects that you want to tag in the drop down list labeled **Apply on**.
8. Select the attribute of the object that will be used to do the matching in the drop down list **Match objects with**.
9. Choose the column of the CSV file whose values match those of the attribute of the object in the drop down **using column**.
10. Check the columns of the CSV file that correspond to the categories that you want to import in the list entitled **Create or update categories with columns**.
11. Optional: Click the button **Select All** to select all the columns at once.
12. Optional: Click **Unselect** to remove the selection from all the columns.
13. Click **Import** to proceed with the importation of tags. A final dialog shows you the number of objects that have been tagged and the problems found during tagging. If needed, repeat the import until you are satisfied with the result.

Related references

- Local and shared (centralized) content

Nextthink Application Library

The Application Library is an online service provided by Nextthink that maintains a knowledge database with security information and classification criteria for applications and web domains.

The Application Library works in collaboration with the Engine to update the fields of some types of objects in a process that is similar to tagging. The difference with tagging is that these fields are always present in the objects. Moreover, the possible values of the fields (the *keywords*) are not defined in a category, but predefined in the Application Library.

The Finder groups the fields that are automatically updated the Application Library under the section **Nextthink Library** of the appropriate objects. To be available, some of these fields require to have installed one of the optional Nextthink Modules. The objects that have such fields are listed below, along with the purpose of each field and an indication of the modules required (if any):

- Binary (Security module)
 - Application category
 - Classify the type of application that owns the binary. Useful to know the kind of applications reports on software usage.
 - Threat level
 - Detection of untrusted and potentially dangerous binaries by comparing their digital footprint with the values of a continuously updated reference database that federates several antivirus applications. Useful for detecting malware.
- Package
 - Windows 7 (32-bit) compatibility
 - Assesses the readiness of installed packages for migration to Windows 7 (32-bit). Useful in workplace transformation projects.
 - Windows 7 (64-bit) compatibility
 - Assesses the readiness of installed packages for migration to Windows 7 (64-bit). Useful in workplace transformation projects.
- Domain (Web & Cloud and Security modules)
 - Threat level
 - Detection of accesses to potentially dangerous web sites by comparing the external domain names with the values of a continuously updated reference database that federates several security providers. Useful for detecting risky web browsing.
 - Domain category
 - Classify the type of web content offered inside a domain. Useful for discovery and browsing profiling.
 - Hosting country
 - Identify the country that hosts the servers of the external domains. Useful for characterization of the traffic and for security issues with blacklisted countries.

Connecting to the Application Library

The Engine must be connected to the Internet either directly or through a proxy to communicate with the Application library:

- The Engine connects to the Application Library within 5 minutes after start up.
- Following this first connection, binaries that have been active at least once in the last seven days are reevaluated every 24 hours.
- For every new binary, package or domain that appears in the system, the Engine takes around 5 minutes to fetch its data from the Application Library.

Configure the Engine to enable or disable access to the Application Library.

Immediate alerts on Application Library fields

As just explained in the previous section, fetching data from the Application Library is not instantaneous. For that reason, immediate alerts that rely on the value of Application Library fields may fail to fulfill their purpose.

For instance, an immediate alert that is configured to detect the appearance of new binaries with high threat level in the system will fail to detect the first execution of such binaries. In effect, soon after the execution of a new binary and its creation in the Engine, the conditions of the immediate alert are evaluated. At that point, however, the Engine has not updated the threat level of the binary yet. It is only around 5 minutes later that the Engine connects to the Application Library and sets the value for the threat level.

Thus, the best practice in this case is to create an hourly alert in addition to the immediate alert and with the same conditions of the immediate alert. In this way, the first execution of a binary with a high threat level may escape the immediate alert, but will be detected by the hourly alert at the end of the current hour interval, once the Engine has set the correct threat level of the binary.

Related tasks

- Enabling and Disabling the Engine Application Library Access

Getting notified by the system

Receiving alerts

Overview

To get notified by the system in the case that a particular situation happens in your IT infrastructure, use alerts. You can receive alerts via email or, in some cases, through the system log of the Appliance. Additionally, you can see the occurrences of service-based alerts in the Portal or those of investigation-based alerts on devices in the Device view of the Finder. To receive alerts via email, configure first the SMTP settings of the Appliance.

Find below a table that summarizes the types of alerts, the potential receivers of the alert and the possible mechanisms to send the alert:

Alert type	Recipient	Sending mechanism
System alert	<ul style="list-style-type: none">• administrator	<ul style="list-style-type: none">• email• syslog
Investigation-based alert	<ul style="list-style-type: none">• Email addresses specified in the definition of the alert• Users that have the alert assigned to one of their roles	<ul style="list-style-type: none">• email• syslog (only global alerts)• Device view (for investigation-based alerts on devices)
Service-based alert	<ul style="list-style-type: none">• Users that add the alert to their Portal• Users that have the alert assigned to one of their roles	<ul style="list-style-type: none">• email• Dashboards My alerts and History in the Portal

Receiving system alerts

Configure the email address of the admin account to receive system alerts. The Engine sends system alerts by email to inform the administrator of the status of the system. Remember that system alerts are predefined alerts that notify special circumstances detected by the Engine, such as internal errors or the expiration of your software license. No user can modify them.

To send emails, the Engine uses the SMTP configuration of the Appliance where it is installed. Only the main administrator receives emails from system alerts. In addition to sending system alerts via email, the Engine logs each occurrence of a system alert in the system log of the Appliance.

Receiving service-based alerts from the Portal

The Portal can generate service-based alerts, which are always related to service dashboards. The triggering of a service-based alerts depends therefore on the results of their corresponding service, as seen by each particular user (their view domain). When a service-based alert is triggered, it appears as active in the special dashboard **My Alerts** of the Portal. In addition, the Portal sends emails to subscribers of the alert both when the alert is triggered and when the alert terminates.

To determine when a service-based alert is triggered and terminated, it is important to know about the *sliding window* mechanism of services. The values of a service are sampled each 10 minutes, but these values are added along one hour intervals for the purpose of generating alerts. Thus, an alert will be triggered or terminated depending on the values collected by its associated service during the last hour.

For example, let us suppose that you set the ratio of devices with errors in a service to 10% and that you create an alert associated to this service. In the next 10 minutes, the service reports that 15 out of 100 devices are in error. Therefore, since the ratio of devices in error is 15% and there was no other previous data available for the last one hour, the Portal triggers the alert associated to the service. Now let us consider the status of the alert depending on the results of the service after the next interval of 10 minutes:

The service reports that no device used it

The accumulated value of the service for the last hour is still 15 devices in error out of 100; the same as in the previous 10 minutes. Therefore, the alert is still active. Following the same reasoning, if no one uses the service for one hour, the alert remains active until the end of the hour,

when the first use reported (15%) lies behind the last hour window. At that point, the alert terminates.

The service reports that 5 out of 100 devices are in error

Supposing that the 100 devices that accessed the service during this interval are the same devices that accessed the service during the previous interval, the accumulated number of devices with error for the last hour are at least 15 (more if the 5 newly reported devices are not part of the 15). The alert is therefore still active.

The service reports that 15 out of 300 devices are in error

Supposing that the 15 devices with error are the same 15 devices with error of the previous interval, and that the 300 devices that accessed the service include the 100 devices of the previous interval, the ratio of devices in error to devices accessing the service becomes now 5%. Since 5% is lower than the threshold of 10% configured in the real-time service widget, the alert terminates immediately.

Another factor to take into account is the minimum number of devices impacted that you configured in the alert. If you set the option **ignore until x or more devices are impacted**, beware that **impacted device** in this context means *device accessing the service* and not *device with error*. In our previous example, the number of impacted devices during the first 10 minutes interval is therefore 100, and not 15.

Finally, it is important to note that the triggering of an alert also depends on the **view domain** of its subscribers. In the same way that the results of a service dashboard depend on the view domain of the user who watches them, a service-based alert is sent to one of its subscribers only if the alert conditions are met within the view domain of that subscriber. That is, service-based alerts are triggered individually per each subscriber and not globally. Using again our previous example, if the value of 15 devices in error out of 100 (15%) was seen by a user with a complete view of the system and another user with a restricted view domain can only see 1 device in error out of 25 (4%), only the first user will receive the alert (>10%).

Moreover, if you have defined multiple **hierarchies** in your setup, each user has a view domain per hierarchy. An alert can be triggered when its conditions are met within any of these different view domains. The actual view domains in which the alert was triggered and their corresponding hierarchy are detailed in the email that the subscriber of the alert receives. Therefore, only one email is sent per alert and per subscriber even if the alert is triggered in multiple domains.

Viewing service-based alerts in the Portal

To see information about the occurrences of service-based alerts in the Portal:

1. Log in to the Portal as a particular user.
2. Click the bell icon in the top right of the Portal window and choose either:
 - ◆ **My alerts**, to see a table with the list of alerts to which you are subscribed and information on their last occurrence.
 - ◇ If an alert is still active, a bell icon is displayed in the first column of the **My alerts** table for that alert.
 - ◆ **History**, to see the past occurrences of the alerts to which you are subscribed.
 - ◇ It is possible to filter the results of the **History** table by hierarchy, alert name, and date by editing the controls on the top right of the dashboard.

In both dashboards **My alerts** and **History**, it is possible to look at the details of an alert, which enable you to break down the results by hierarchy levels:

1. Hover the mouse over the name of the alert in an entry of the table and an info icon (a little **i** with blue background) appears to its right.
2. Click the info icon to see the details of the alert.
3. In the dialog with the details, select the desired hierarchy from the list **Display impact data for hierarchy**.
4. Select a level of the hierarchy from the list **Hierarchy level** to get the results of the alert for a particular level only.
5. Optional: Click the right pointing arrow with the label **CSV** at the bottom right corner of the table to export the details of the alert to a CSV file.

Receiving alerts linked to roles

Even when you do not create alerts yourself, you can receive alerts that are assigned to you by the roles attributed to your user account. You cannot modify or delete any of the alerts that are linked to your roles. The alerts that can be linked to roles are of two types:

- Investigation-based alerts
- Service-based alerts

To see the investigation-based alerts that are attributed to you according to your roles:

1. Log in to the Finder with your user account.

2. Click the **Settings** section of the accordion on the left-hand side of the Finder.
3. Inside **Settings**, select **Role-based alerts** from the drop down list labeled **Section**. For each one of your roles, you see a folder holding the alerts that correspond to the role.

Moreover, in the Device view of the Finder, there is a separate alert timeline for each one of your assigned roles. Alerts on devices that are attributed to you because of your roles are displayed there.

To see the service-based alerts that got assigned to you because of your roles:

1. Log in to the Portal with your user account.
2. Click the bell icon in the top right corner of the window.
3. Select the dashboard **My alerts**.
4. There you have the list of the alerts that you added to your Portal or that were automatically added because they are mandatory for at least one of your roles. You can see if the alert is linked to a role in the last column.

Related tasks

- Sending email notifications from the Appliance (Configuration)
- Creating a service-based alert
- Creating an investigation-based alert
- Defining user roles

Related concepts

- Alert

Creating a service-based alert

Service-based alerts rely on the thresholds of the services that you define in the Finder. The prerequisites for a service to accept the creation of an alert are thus the following:

- The service must be active (i.e. not disabled).
- The service must specify thresholds in its definition.
- There is no other service-based alert defined for the same service.

To create a service-based alert in the Portal:

1. Log in to the Portal as admin.
2. In the **ADMINISTRATION** top menu, under **CONTENT MANAGEMENT**, select the **Alerts** dashboard.
3. Click the plus sign on the top right corner of the **Alerts** dashboard. The dialog to configure a new service-based alert pops up.
 1. Type in the **Name** of the alert.
 2. Optional: Describe the function of the alert briefly in the **Description** field.
 3. Assign the alert to a category or create a new category for alerts in the **Category** section.
 4. In the **Service** list selection, pick the service that you want to use as a base for the alert. Only the active services that specify thresholds in their definition and that are not used in any other alert are available. The dialog displays the thresholds configured for the service as well as the box **ignore until x or more devices are impacted**, since they are used to determine when to trigger the alert.
 5. If the service defines two thresholds, choose the one that triggers the alert in **Trigger alert when x threshold is crossed**:
 - ◇ Select **yellow** to trigger the alert when the ratio of the devices with an issue over the devices using the service exceeds the warning threshold.
 - ◇ Select **red** to trigger the alert when the ratio of the devices with an issue over the devices using the service exceeds the error threshold.
 6. Tick the **Send email when alert is triggered** check box to send the details of the alert to its subscribed users via email.
4. Click **Create** and your new alert is added to the list of alerts under administration.

The alert is now created, but it is not enabled until users subscribe to it. Users may subscribe individually to an alert if the alert is part of their roles. If a role includes an alert as mandatory, all the users who have that role assigned are automatically subscribed to the alert.

To subscribe to a service-based alert:

1. Log in to the Portal with your user account.
2. Click the bell icon in the top right corner of the Portal.
3. Click the entry **My alerts** from the drop-down list.

4. Click the plus sign icon followed by the label **Subscribe to alert** in the top right of the special dashboard **My alerts**.
5. Select one or more alerts from the list **Alert**. The list shows only the alerts that are not yet added to your Portal. If there are no alerts that you can subscribe to, the dialog displays an appropriate message and finishes.
6. Optional: Filter the list of alerts by role with the help of the drop-down list **Filter by role**. This is useful for locating a particular alert in the list when many alerts are defined for your roles.
7. Click the button **OK**. The alert is added to the special dashboard **My alerts**.

Related tasks

- Receiving Alerts from the Portal
- Adding users
- Creating a service

Creating an investigation-based alert

To define your own alerts on any kind of object, use investigation-based alerts. As their name indicates, investigation-based alerts express their triggering condition in the form of an investigation. The Engine periodically executes the investigations associated to alerts, depending on the frequency specified for each alert.

You can create an investigation-based alert by either:

- Defining the alert from scratch.
- Using an existing investigation as starting point.

The dialog to create alerts in the Finder is very similar to the dialog for designing investigations. There are a couple differences though:

- Investigations associated to an alert must be based on objects. You cannot associate an investigation based on activities or events to an alert.
- The time frame of the investigation depends on the frequency of the alert. You cannot specify a different time frame in the dialog for designing the investigation.
- An additional section at the end of the dialog for alerts let you specify the criticality, the frequency and the action to take when the alert is triggered.

Creating an investigation-based alert from scratch

To create an investigation-based alert from scratch:

1. Log in to the Finder.
2. Go to the **Settings** section in the accordion.
3. Inside the **Settings** panel, click the drop down list **Section** and either:
 - ◆ Select **Global alerts** to create an alert visible to every user. This option is only available if your account has the right privileges to create global alerts. Currently, every user can see global alerts only in the timeline of the Device view. The investigation of the alert must therefore be based on devices for the alert to be visible in the Finder.
 - ◆ Select **My alerts** to create an alert that is visible to you only in the Finder. This option is available to every user. If the alert is based on devices, it is displayed in the timeline of the Device view.
4. Right-click the area of the section and select **Create new alert** or type **Ctrl+N**. The dialog for designing a new alert shows up.
5. Enter a name for the alert by replacing the default **Untitled alert x** at the top of the dialog.
6. Optional: Type a brief description of the alert below the name.
7. Edit the investigation part of the alert as any other investigation, with the restrictions that you must retrieve an object and not an activity or an event and that you do not have to specify the time frame. After specifying the attributes to display, you reach the specific **ALERT** section.
8. Set the level of the alert in the drop down list **Criticality**:
 - ◆ Select **Normal** for non-critical alerts. Normal alerts based on devices are displayed in yellow in the timeline of the Device view.
 - ◆ Select **High** for critical alerts. Critical alerts based on devices are displayed in red in the timeline of the Device view.
9. Specify the frequency with which the system will check the conditions to trigger the alert:
 - ◆ Select **Immediate** for the system to check the conditions that trigger the alert almost continuously (every 30 seconds). Due to the nature of immediate alerts, you cannot select many display attributes that are usually available for the investigation. The Finder warns you when you select a display attribute that is incompatible with immediate alerts by showing a red cross to the right of the **Immediate** keyword. Hover the mouse cursor over the red cross to see the list of incompatible attributes that you selected. To avoid flooding, one hour must elapse between two consecutive immediate alerts for the same object.

- ◆ Select **Hourly** to evaluate the conditions 15 minutes after the end of every hour and get the results for the whole hour that just passed by.
 - ◆ Select **Daily** to evaluate the conditions 15 minutes after midnight every day and return the results for the past day.
 - ◆ Select **Weekly** to evaluate the conditions 15 minutes after midnight every Monday and send the results of the investigation for the last week.
10. Choose the action to take when the alert is triggered. Note that the results of an investigation-based alert are limited to a maximum of 250 objects with 15 attributes per object. Results exceeding these values are cut down to avoid sending too much data.
 - ◆ Check **Send syslog** to write the results of the investigation associated to the alert to the system log of the Appliance. This option is only supported by global alerts.
 - ◆ Check **Send e-mail** to send the results of the alert by email to selected recipients. Note that any recipient can receive both global and non-global alerts.
 11. Click **Save & Run** to save the new alert and run the associated investigation.

Creating an alert from an existing investigation

To create an investigation-based alert from an existing investigation:

1. Log in to the Finder.
2. Find the desired investigation in the accordion.
3. Right-click the name of the investigation and select **Add to My alerts...** (or **Add to Global alerts...** if you have the right privileges). The dialog to design the alert shows up with the data of the investigation prefilled, so you only need to fill the **ALERT** section.
4. Optional: Change the name of the alert at the top of the dialog. By default, the alert borrows its name from the investigation.
5. Optional: Change the description of the alert that you find below the name. By default, the description of the alert is inherited from the investigation as well.
6. Set the criticality, frequency and actions of the alert as described above.
7. Optional: Modify the investigation settings to meet your needs. The original investigation is not modified.
8. Click **Save & Run** to save the alert and execute the associated investigation.

Limit on the number of alerts

Using the methods described above, you can create and enable up to a maximum of 50 global alerts. For their part, users can create (or receive from their roles) and enable up to 10 additional local alerts per account on each Engine.

The total number of enabled alerts in an Engine, including the global alerts and the local or role-based alerts of all users, is limited to 150 alerts.

Building web-based dashboards

Introducing dashboards in the Portal

Overview

Build web-based dashboards in the Portal to readily present the information about your IT infrastructure that interests you the most. Use indicators, tables and line charts to display real-time and historical data related to activities, objects, license use, and IT services within your corporate network.

Thanks to the web-based dashboards of the Portal, quickly find out those parts of your IT infrastructure that are working well and those that may require your attention. Hardware and software issues, network issues, or service degradation are all instantly apparent in properly designed Portal dashboards. The historical data stored in the Portal make dashboards an ideal tool to follow the progress of *change and transformation* projects as well.

Types of dashboards

Dashboards are grouped into modules. The type of a module determines the type of dashboards that it can hold. There are three types of modules:

Blank module

A blank module holds dashboards based on metrics. The dashboards of blank modules are highly customizable, letting you mix different metrics and distinct visualizations (*widgets*) for those metrics in the same dashboard. Combine carefully the widgets and metrics in a dashboard to get the most complete and consistent view possible on a topic of interest.

Service module

A service module holds dashboards based on services. Each dashboard in a service module represents a different service. Because service-based dashboards are not as customizable as metric-based dashboards, they are even easier to create. A predefined set of widgets gives you a variety of points of view on the service: the number of devices using the service, the network traffic generated, the issues related to connectivity or software malfunction, etc.

Software metering module

A software metering module holds dashboards that assess the use of software licenses within your company. Each dashboard presents you with

information about the number of installations and actual use of a particular application, relating this information with the number of licenses available.

Dashboards and hierarchies

Take advantage of your existing hierarchies when working with dashboards. The Portal automatically compute dashboard results for every level in your hierarchies. When viewing a dashboard, choose a node of the current hierarchy to display information that only applies to that particular node. A well-designed hierarchy can greatly help you locate the source of problems within your network.

Creating a dashboard

Overview

Create a new dashboard in the Portal whenever you wish to get a visual representation of a part or an aspect of your IT infrastructure. Dashboards summarize a lot of data and complex investigations in a single web page; therefore, they are most useful when built with a consistent set of graphical items.

Administrators of any kind can create local content in the Portal in the form of dashboards. Normal users whose profile lets them create personal dashboards can equally create their own content.

Portal dashboards are organized into modules, which act as containers for dashboards. The type of module determines the kind of dashboards that the module may hold.

Creating modules and dashboards

To create a dashboard, you need a module first. Depending on the kind of content that you want to add to the dashboard, the module must be of an appropriate type.

Follow the instructions in the corresponding section of the documentation to create or reuse a module of a particular type and add a new dashboard to it:

- To follow the evolution of *metrics*, choose a module of type **Blank**.
- To follow the evolution of *services*, choose a module of type **Service Monitoring**.

- To keep the usage of *software licenses* inside your company under control, choose a module of type **Software Metering**.

Related concepts

- Dashboard

Examining metrics in depth

Overview

When displaying metric values in the widgets of a dashboard, you may be interested in knowing which objects are behind the numbers. For any figure in a dashboard that represents a count metric, it is possible to see the objects that added up to the total. The list of these objects is called the *details* of the metric. If you selected grouping options or additional display fields when creating your metric, they are displayed in the details.

Displaying the details of count metrics

To display the details of a count metric from a dashboard:

1. Find in the dashboard a widget (KPI or table) that displays the metric. It is not possible to show the details of a metric from a line chart.
2. Hover the mouse over the figure. A small speech bubble shows up.
3. Click **Show details** in the bubble. The list of the objects that added up to the count metric is displayed.
4. Optional: If the list of objects is too big to fit in the dialog, use the controls at the bottom left of the dialog to move through pages. There is a limit to the maximum number of objects that the Portal can display in the details. If the limit is reached, the dialog indicates it with an appropriate message.
5. Optional: Click the arrow link with the label **CSV** at the bottom right corner of the window to export the list as a CSV file.
6. Click **OK** once you are done to close the dialog and return to the dashboard.

In table widgets, if you have grouped the results of the count metric, you exactly get the list of objects that correspond to the clicked figure, according to the grouping options for breaking down the results.

Note that service dashboards do not have the option to display details. Showing the details is only available in dashboards based on metrics.

By default, the Portal stores the details of count metrics for the current day, week, month, and quarter. To keep historical data for previous periods, reserve additional disk space for the Portal.

Related references

- Types of widgets
- Data retention

Assessing license use

Overview

Check the license compliance for a set of programs by measuring their real utilization. Compare the number of installed programs with the number of purchased licenses and save license costs for programs that are rarely used or, in the opposite case, allow some budget to purchase additional licenses.

To examine the use of program licenses within your company, first create a *software metering metric* for each product of interest. Then add to your dashboards one or more software metering modules to display the previously defined metrics. Software metering modules help you automate the assessment of software licenses across your hierarchies.

Applies to platforms:

Creating software metering metrics

Unlike other types of metrics, which are created in the Finder, software metering metrics are created in the Portal.

To create a software metering metric:

1. Log in to the Portal as administrator.
2. From the top drop-down menu **ADMINISTRATION**, select **Software metering metrics** under **CONTENT MANAGEMENT**.
3. Click the plus sign at the top right corner of the dashboard. The dialog to create a new software metering metric shows up.
4. Type in a name for the metric under **Name**.

5. Optional: Describe the purpose of the metric under **Description**.
6. Click **Continue**. The dialog starts retrieving the list of available programs from the Engines linked to the Portal while displaying the message **Fetching programs from Engines**. Once the process is finished, the dialog is ready for you to configure the programs to assess in the **Programs** table.
7. Type the number of days in the past to measure program utilization in the box **for the last x days**. By default, the number of days is 30.
8. Click **Add program** to define how to audit a new program. A new dialog appears to let you set up the program and its licenses.
 1. Step 1 of adding a program: identify the program
 1. Type a name to identify the program in the entry **Program label**. Each program name must be unique in the metric.
 2. Optional: Enter a web address with additional information about the program in the entry **Add an external link to program's informations**. Use, for instance, the official web page of the vendor of the program.
 3. Choose how to select in the next step the packages that correspond to the program:
 - To pick the packages from a list proposed by the widget, select **from the list**.
 - To provide an investigation which will pick the packages for you, select **corresponding to investigation**.
 2. Step 2 of adding a program: identify the packages
 1. Depending on the mode that you selected in step 1 to select the packages, you either:
 - Choose one or more packages from a list. If you have a mixed installation of Windows and Mac OS devices, the list displays packages from both platforms. Only installed packages are shown in the list:
 1. Filter the list of packages by choosing the initial letter of their name in **Available packages starting by**.
 2. Click the name of one package (or more while maintaining the **Ctrl** key pressed).
 3. Click **Add to selected** to add the packages to your selection.
 4. Optional: By default, all versions of the packages selected are accounted for license use. If needed, choose a specific version of a package by clicking the pencil icon to the left of the name of the package in the list of selected

- packages. Type in a particular version in the **Edit package version** dialog and click **Edit**.
5. Click **Next** to move on to step 3 of the wizard.
- Alternatively, use an investigation on packages:
 1. Export an investigation based on packages from the Finder to the clipboard.
 2. Paste the investigation in the text area under the label **Paste an investigation**.
 3. Click **Next** to move on to step 3 of the wizard.
3. Step 3 of adding a program: configure licenses
 1. Choose the level of the hierarchy through which you want to distribute the licenses in **Set licenses on level**. Remember that all the licenses must be distributed over nodes at the same level in the hierarchy. Therefore, the chosen level remains valid for all the licenses that you add to the metric.
 2. Click **Add license** to configure a new program license. The dialog for adding a license pops up.
 3. Type a name to identify the license in the entry under the label **Reference**.
 4. Optional: Type a brief description of the license in the text area **Description**.
 5. Optional: Type in the number of purchased licenses in the entry labeled **Quantity**. Leave it blank if you have an unlimited set of licenses.
 6. Optional: Enter a date in the section **Expires on** to specify the time validity of your license. If you leave it blank, the license never expires.
 7. Optional: Pick a node to which licenses apply from the **Node** list. The nodes that you can pick belong to the hierarchy level that you selected before.
 8. Click **Add** to finish adding the license.
 4. Step 4 of adding a program: specify binaries
 1. For the metric to compute statistics about program usage, you may pick a set of binaries which are related to the selected packages in the **Significant binaries** section:
 - Choose **no significant binary** to avoid this step altogether.
 - Choose **based on a list** to create a list of binaries. If you have a mixed installation of both Windows and Mac OS devices, you can add binaries of both platforms to the list.
 1. Click **Add binary** to add a new binary to the list. A dialog for adding binaries appears.

2. Type in the exact name of the executable program in **Executable name** (include the .exe extension if it is a Windows binary).
3. Type the first numbers of the versions of the executable that will be taken into account for computing the statistics in **Version starts with**.
4. Click **Add** to add the defined binary to the list.
- Choose **based on investigation** to automatically select significant binaries from an investigation.
 1. Export an investigation based on binaries from the Finder to the clipboard. The investigation can be multi-platform.
 2. Paste the investigation to the text area below the option **based on investigation**.
2. Set the threshold of daily average usage of binaries per device to consider only those binaries that a device actually executes for a significant amount of time. Select the number of hours and minutes in **Under usage threshold**.
3. Click **Add** to end the wizard for adding programs.
9. Click **Finish** to end up the edition of the metric.

Right after adding a new software metering metric, optionally launch its computation in the Portal. Otherwise, software metering metrics are processed during the nightly computation of the Portal, as any other metric.

Creating a Software Metering Module

Once you have defined one or more software metering metrics, create a software metering module to visualize them in your dashboards.

To create a software metering module:

1. Log in to the Portal as administrator.
2. Click the menu icon in the right-hand side of the blue ribbon at the top of the window.
3. Select the option **Create new module....** The dialog to create a new module shows up.
4. Choose **Software Metering** as the type for your new module.
5. Select the software metering metrics that you wish to include in your module from the list of **AVAILABLE** metrics. Use the **Ctrl** or **Maj** keys while you click with your mouse to select more than one metric at the same time.

6. Click the left-to-right arrow to move the selected metrics from the **AVAILABLE** list to the **SELECTED** list.
7. Click the button **Create** to generate a new software metering module with the selected metrics.

Interpreting the results of software metering metrics

To view the results of a software metering metric, navigate to the software metering module that holds the metric (the module must lie within your available dashboards) and select the dashboard that displays the metric of interest.

The dashboard of the metric shows a table with license compliance info that can be broken down both by software product and by hierarchy level. By default, the table displays an overall view of all the products located at the hierarchy level that corresponds to the view domain of the user (for instance, if the user is a central administrator, that would be the root level). In the overall view, you get the following columns in each row of the table:

- A circular bullet whose color indicates the status of license usage:
 - ◆ **Green** when the number of installations of a particular software product are equal or lower to the number of valid licenses for that level of the hierarchy.
 - ◆ **Red** when the number of installations of a software product exceed the number of valid licenses available for the level.
 - ◆ **Gray** is only used when you are viewing the results on nodes that do not belong to the hierarchy levels that you chose in the configuration of the licenses. For instance, if you configure the number of valid licenses only at the root (top) level of the hierarchy, you will see gray circles when you break down the results to lower levels, because you have not provided license information specifically for those levels.
- The name that identifies the program in the column **Product**.
- The number of devices that have the program installed in the column **Installed**.
- The number of valid licenses for the program in the column **Nb valid licenses**.
- The ratio of devices with the program installed divided by the number of valid licenses in the column **Compliance**.
- The number of devices that underutilize their licensed products in the column **Nb devices in under usage**.

Navigating through products and hierarchy levels

If you configured more than one software product in your metric, you can select one of the products to see the license information broken down by hierarchy. At the top left of the dashboard, choose a program from the **Product** drop-down list to show the results for that particular product. Alternatively, hover the mouse cursor over the name of the product in the table and click the down arrow that appears to its right.

The **Product** column of table is then replaced by a column with the name of current hierarchy level, filled with the names of the nodes in that level. For each hierarchy node, the table displays the license status of the product with the color codes seen above.

To go down in the hierarchy, use the drop down list for the hierarchy that is placed to the right of the **Product** drop-down list. Select one node from the drop-down and the table will adapt to present the results in the chosen hierarchy level. Alternatively, you can hover the mouse cursor over the name of a node in the table and click the down arrow that appears to its right.

To go back to a higher level in the hierarchy, there is a navigation tool over the **Product** and hierarchy drop-down lists that displays the whole hierarchy path of the current level. Click the name of the desired level/node in this navigation tool to move to that level and update the table results accordingly. If you defined more than one hierarchy, the navigation tool also lets you choose the particular hierarchy according to which you want to assess the use of licenses. To switch from one hierarchy to another, click the name of the current hierarchy in the navigation tool and select the hierarchy to replace it from the drop-down list. Of course, if you just defined one hierarchy, no drop-down list shows up.

Analyzing binary usage

If you configured the metric to survey significant binaries, you can get detailed information about the use of those binaries on the monitored devices. Only those devices with the appropriate packages installed that have been active for the last 30 days are included in the computation.

To get statistics about binary usage:

1. Hover the mouse cursor over the results of the **Installed** column. A small info icon appears to the right of the value.
2. Click the info icon and the widget displays the **Details** table, with the list of devices where the program is installed.

3. Select the type of information that you want to see from the list in the top left of the widget above the table. Choose between:
 - ◆ **Binary usage**: for each configured significant binary, the table shows whether the binary was actually used in the device or not.
 - ◆ **Statistics**: the table displays the cumulated average usage and the average executions per day of all significant binaries, as well as the time of their last activity for each one of the involved devices. For devices that did not execute any significant binary during the last 30 days, the average usage displays:
 - ◇ **0 ms**, if the device was active during the last day (the day of the computation).
 - ◇ - (a dash sign), if the device was not active during the last day.
4. Optional: Click the link **CSV** at the bottom right corner of the **Details** dialog to export the results to a CSV file.

The info icon also shows up in the column of underused devices. As expected, clicking on it gives you the details of underused devices only.

Computing dashboard data

Overview

The Portal employs different techniques to retrieve and process dashboard data from the connected Engines. Depending on their mode of activation, the techniques for computing dashboard data can be classified as automatic or manual:

- Automatic computations
 - ◆ Computation after metric creation
 - ◆ Nightly computation
 - ◆ Real-time computation (live service data)
- Manual computations
 - ◆ Launch computation of metric from the Finder
 - ◆ Launch computation of software metering metric from the Portal

In this article learn about the different types of computations, how to manually launch the computation of metrics from either the Finder or the Portal, and how to track the status of computations from the Portal. Learn also about the consequences of computing the values of a metric for dates in the past.

Automatic computations

Computation after metric creation

When you create and save a new metric in the Finder, it automatically launches its computation for the past day. A newly created metric has thus one day of history unless you clear the metric manually.

Nightly computation

The nightly computation is the main source of dashboard information for the Portal. It usually takes place during the night (hence its name), when the load on the Portal and on the Engines is lower because users seldom connect at night. At the scheduled time, the Portal starts collecting data related to the enabled services and metrics in all connected Engines and processes it for being displayed in the dashboards. This automatic computation is scheduled by default at 1 am local time, but this time is configurable.

Thus, every night the Portal collects the accumulated data in the Engines for the past day. In the case of metrics whose history is missing for some consecutive days including the last day, the Portal computes not only the past day, but the number of days configured.

Real-time computation

When displaying live data in service dashboards, the Portal continuously receives data from the Engines about the current status of the services. This automatic computation requires no special configuration.

Manual computations

Manual computations do not replace the nightly computation of the Portal, but are a complement to it. Manually computing a metric is specially useful when you create or modify a metric. Instead of waiting for the nightly computation to get the results for the metric, you can manually trigger its computation to see how it looks in the Portal.

Metric computation from the Finder

To trigger the computation of metrics from the Finder:

1. Right-click the name of a metric or of a folder holding metrics in the left-hand side accordion.

2. Select **Compute** from the context menu:
 - ◆ Choose **For the last day**, to compute or recompute the results of the metric (or metrics) for the day before.
 1. A dialog warns you that the operation will clear the history of the metric (or metrics) for the last day. Click **Yes** to proceed.
 2. A final dialog informs you that the computation of the metric (or metrics) will start shortly. Click **OK**.
 - ◆ Choose **Over the maximum available period**, to compute the metric (or metrics) for all the past days available in each connected Engine.
 1. A dialog warns you that the operation will clear **all the history** of the selected metric (or of all the metrics in the selected folder). Click **Yes** to proceed.
 2. A final dialog informs you that the computation of the metric (or metrics) will start shortly. Click **OK**.

Beware of the option to recompute metrics over the maximum available period. It really clears **all the history** of metrics. For instance, if you have three months of historical data in the Portal for a particular metric and two weeks of data available in the Engine, asking to recompute the metric over the full period will erase the three months of history and recreate only two weeks. Therefore, use this option with care and only when the modification of a metric completely invalidates previous results. Keep in mind as well that the recomputation of metrics for past days suffers from some limitations.

Software metering computation from the Portal

When creating a new software metering metric in the Portal, you are given the option to compute the metric for the last day immediately after its creation.

To compute software metering metrics that are already created:

1. Log in to the Portal as administrator.
2. Click the **ADMINISTRATION** item in the top menu.
3. Select **Software metering metrics** under **CONTENT MANAGEMENT** in the drop-down menu.
4. In the list of available metrics, tick the box in the first column for each metric that you want to compute. Alternatively, tick the box at the top of the list to select all available metrics at once.
5. Click the sprocket icon placed in the top right corner of the dashboard. A dialog informs you that the computation will be done for the last day.
6. Optional: Tick the box in the dialog to overwrite current data; that is, to clear and recompute as well those metrics that already have results for the

- last day.
7. Click **OK** to schedule the computation. Another dialog informs you that the computation is scheduled and that you can track it.
 8. Click **Done**.

As any other metric, software metering metrics are also computed during the nightly computation of the Portal.

Tracking computations

To track the computations of metrics in the Portal:

1. Log in to the Portal as administrator.
2. Click the **ADMINISTRATION** item in the top menu.
3. Select **Computations** under **CONTENT MANAGEMENT** in the drop-down menu.

The **Computations** dashboard has two modes for displaying computations. Select the mode from the list labeled **Display** in the top-right corner of the dashboard. Choose between:

- **all computations** (default): display the list of all the computations launched during a specific time interval.
- **automatic computations**: display historical statistics of the nightly computations as line charts.

All computations mode

When set to the **all computations** mode, the **Computations** dashboard displays a table that includes both the manual and the automatic computations launched today by default. Filter the results by selecting other time frames and the user who initiated the computation from the two lists interleaved in the following sentence that you find at the top of the table:

- **Display computations for -time frame- created by -user.**

As time frame, choose among:

- **today** (default)
- **last week**
- **last month**

To filter by the user who launched the computation, choose among three options:

- **everybody** (default): list all the computations, no matter who initiated them.
- **myself**: list only the computations initiated by the current user.
- **Nexthink Portal**: list only the nightly computations initiated by the system itself.

The table shows the current status of each computation within the selected time frame, including (when applicable) its start time, end time, progress ratio, duration, and owner. The dashboard content is automatically refreshed every 10 seconds.

It is possible to stop a scheduled or running computation. Administrators can stop only those computations initiated by themselves. Central administrators, on the other hand, can stop computations initiated by anyone. If you stop a computation during its execution, the results for those dates that have been fully computed are saved and the rest are discarded.

The following table describes the possible computation statuses:

Icon	Name	Description
	Scheduled	When a computation is scheduled, the operation has been submitted and put in the queue. There is no ongoing computation yet; therefore, there are no details about progress, time, or duration, but the computation can be cancelled.
	Running	The computation is currently being performed. The start time and progress fields are available. The computation can be cancelled.
	Completed (success)	All metrics were computed without error. Details about the computed metrics are available.
	Completed (failure)	Errors occurred during the computation. Some metrics may have been computed correctly but at least one had an error. Details show the completed and failed computations of the metrics.

	Cancelled	The computation has been manually cancelled. Details may show some metrics that have been completely computed before cancellation (with or without errors), while other metrics have not been computed.
--	-----------	---

Display the details of all finished computations (either completed or cancelled) by clicking the information button.

Automatic computations mode

This mode of the **Computations** dashboard displays the evolution of nightly computations through time for the last 90 days.

The line chart arranges 5 different values:

- **Total duration** is the duration of the computation. Note that if an error happens during the nightly computation, the Portal may make a new attempt to recompute. In the previous mode, all attempts are displayed individually; in this mode though, attempts are aggregated to have only one duration value per day. Therefore, the duration is the sum of all attempts.
- **Operations performed** is the total number of calculations made in the Portal. It aims to represent the workload of each nightly computation. The number of operations is calculated as the number of metrics multiplied by the number of days to compute. Skipped metrics are not counted in. The value is useful to explain differences in duration from one day to another.
- **Attempts needed** is the number of attempts that were necessary to

complete the computation. The number of operations and the number of attempts explain the total duration.

- **Metrics successfully computed** is the number of metrics computed without error. A metric is successfully computed if all the days have been correctly computed, even if the Portal needs multiple attempts to achieve it.
- **Metrics unsuccessfully computed** is the number of metrics whose computation failed. A metric is unsuccessfully computed if, after all attempts, at least one day could not be computed.

Hovering the mouse over the line charts lets you see the values for a particular date. Click to see the details for a particular day.

Click the info button to the right of a value for displaying the details of the last nightly computation filtered by that value. For example, to see the details of successfully computed metrics for the last computation, click the info button to the right of the value **Metrics successfully computed**.

Computation details

To get details about a specific computation in the **Computations** dashboard:

- Click the info button in the table, when the display mode is **all computations**, .
- Click any point in the line chart (or the info button to the right of a value), when the display mode is **automatic computations**.

The details dialog displays the list of metrics with their individual computation status. You can only see the details of those metrics that fall into your administration domain.

In the **all computations** mode, the table displays individual computations, including manual computations and separate attempts of nightly computations. Therefore, when you open the computation details from this mode, the date is fixed and there is no selection of attempts. On the other hand, when opening the details of a nightly computation from the **automatic computations** mode, it is possible to select a different date for convenience and see a different. In addition, if multiple attempts were needed for the nightly computation of the selected date, you can also select the specific attempt. Thus, when opening the details dialog from the **automatic computations** mode, find these additional selectors:

- **Display details for** *-date*: to select a particular date.
- **This computation required multiple executions. Display** *-attempt*: to select a particular attempt.

In both modes, the dialog lets you choose the metrics for which you want to see the details, depending on the status of their computation:

- Completed (successfully or not, but not skipped)
- Skipped
- Successful
- Unsuccessful

For unsuccessfully computed metrics, click the cross icon to display the error that stopped the computation.

Widgets with no data

If the Portal has not computed data for a metric on a particular date, the widgets that display the value of the metric show it in different ways depending on their visual appearance:

- In KPI or table widgets, the value of a metric with no data is represented with a dash (-) character.
- In line charts, when hovering the mouse over the points where the metric was not computed display the message **no data computed**.

In the widgets of service dashboards, you find the same behavior when there is no data for the service. Similarly, in the overview dashboard of a service module, a dash character representing the status of a service indicates a lack of data for that particular service.

Note that you still may see live data in a service dashboard that received no data from nightly computations. For instance, the first day that you create a service, you may see live data for that service, but you will get no data for the service if you navigate to a previous date.

Computing metrics for dates in the past

There are a few cases where you may want to compute the value of metric for a date in the past:

- You create a new metric and you want to compute its value for some days before its creation.
- You modify a metric in such a way that it completely invalidates previously computed values. You may want to clear the history of the metric and recompute it for some days in the past.
- The nightly computation of the Portal failed for some reason at a specific date and you want to have the value of a metric for that date.

You can either trigger the computation of a metric manually from the Finder or wait for a new nightly computation of the Portal. In the case of newly created metrics, only manually triggering the computation will do, because they automatically compute the last day at the time of creation, preventing thus the Portal from going further to the past. Remember that the nightly computation automatically recomputes the metrics up to the configured number of past days,

if the data of the metrics are missing for some consecutive days including the last day. The nightly computation will not automatically fill in the gaps though if the failed computations are placed between successful computations.

Regardless of computing the metrics manually or automatically, you must be aware of the limitations of computing metrics for dates in the past.

Metrics may include in their computation values of objects (or conditions on these values) for which the Engine does not keep a historical record. Examples of these values may be the free disk space or the antivirus status of a device. During the nightly computation, the Portal takes the current value of those fields to compute the metrics for that day. In this way, the Portal always uses the most recent values to compute the metrics for the last day.

When computing the metrics for past dates, however, the Portal does not know the values of these fields in the past, so it still uses their most recent values. Since these fields usually do not change quickly over time, the computed values are often a good approximation, but if the value has a significant change (for instance, the antivirus real-time protection goes from *on* to *off*) the value of the metric may be wrong.

Therefore, beware of computing metrics for dates in the past when the metrics depend on values of fields for which the Engine does not keep a historical record.

Related tasks

- Changing the nightly computation time of the Portal

Related references

- Widget Compute State In Charts

Reusing dashboard content

Overview

Administrators of any kind can publish Portal content for other users to share the same dashboards. The unit of sharing is the module; therefore, when a module is published, it is shared with all the dashboards and widgets that it holds.

Nevertheless, not all the users are able to see all the published modules. Users can see a particular published module only according to specific rules that depend on the users' type, their administration domain (if they are administrators), and their roles.

Publishing a module

You need to be an administrator to publish a module. To publish a module, first create the module or modify an already published module by copying it to your personal content. To make a local copy of a published module in the **PERSONAL** section:

1. Log in to the Portal as administrator.
2. Click the module navigation tool in the left-hand side of the dark blue ribbon.
3. Open the published module. Either:
 - ◆ Click the name of a module under a section corresponding to one of your assigned roles in **My content**.
 - ◆ Click the name of a module in **All published**.
4. Click the menu icon in the right-hand side of the dark blue ribbon.
5. Select the option **Copy module to my content**.

Note that normal users (non-admin) can also copy a module included in their roles to the **PERSONAL** section, as long as they have the permission to create their own modules. However, later they cannot publish the modules that they create or modify.

Once you have created the new module or modified an existing module, publish it:

1. While viewing the module content in the Portal, click the menu icon in the right-hand side of the dark blue ribbon.
2. Under the section **MODULE**, select the option **Publish module...**. A dialog shows up.
3. Publish your module as new or substitute an existing module. Choose between:
 - ◆ **Create new module**. Type in a name for the module that is not repeated. Note that, in the list of existing modules, you do not see the names of those modules that were created by administrators with a different administration domain. Therefore, there can be a name conflict even if you do not see the name that you chose for your module in the list.

- ◆ **Replace existing module.** Note that you can only replace those modules created by you or by other administrators with the same administration domain.

1. Choose the module to replace from the list.
4. Optional: Tick the box **Keep a copy in my personal content** if you do not want the module to disappear from your **PERSONAL** section after publishing.
5. Click **Done** to actually publish the module.

After publishing the module, you can assign the module to a role.

Seeing a published module

Normal users see only those published modules that are included in their roles. Administrators however see, in addition to the published modules included in their roles, the modules published by themselves and by other administrators whose administration domain is at the same or a lower level in the hierarchy in the **All published** group.

For example, central administrators are placed at the highest level in the hierarchy; therefore, they are able to see the modules published by any other administrator. Note however that only the administrator that published a module or administrators at the same level in the hierarchy are able to replace the published version of the module. The other administrators that see the module can still copy it to their content and modify it locally. Additionally, administrators at a higher level in the hierarchy can delete the published module, but not replace it.

Find the summary of permissions and access rights for Portal users.

Related tasks

- Adding users

Related references

- Access rights and permissions

Importing and Exporting authored content

Methods for reusing authored content

Overview

There are some situations when you want to share with others the content that you have created either in the Finder or in the Portal. Within a normal setup (that is, an installation with one Portal and several connected Engines) you can create some type of content that is instantly shared by other users of the system. This is the case, for instance, of *centralized* content created with the Finder or of content associated to roles.

Manual import/export in the Finder

Other kind of content that you create in the Finder is local to each Engine. To share local content, first connect to the Engine holding the elements to share with the Finder and export them manually, then connect to the target Engine to import them back. This manual method is also valid for exporting local or centralized content to Engines in different setups, as long as dependencies are respected. For instance, to export an investigation that uses in its conditions a category that is not present in the target Engine, you must import the category beforehand.

Publishing modules

The Portal has its own way of sharing content among different users: administrators can publish the modules that they create, and optionally assign them to roles, so that other users can profit from them. This method however does not let you take content from one Portal and import it into another Portal. This latter scenario typically occurs when you have separate pre-production and production environments.

Content packs

To export a coherent set of Finder and Portal elements at the same time, use content packs. A content pack groups in a single file multiple items of Finder content and Portal modules. For instance, recalling our dependency example above, you can include in a same content pack an investigation and the categories on which the investigation depends. Similarly, when exporting Portal modules, you definitely want to include in the same content pack the metrics and

the services on which the modules depend. See in the following articles how to import content packs or make your own content packs.

Nextthink Library

Ready-made content packs are available from the Nextthink Library. The packs in the Library are designed to provide you with customizable solutions for different IT areas: security, transformation, compliance, etc. The method to import a library pack is different from importing a content pack from a file.

Related tasks

- Reusing dashboard content
- Adding users (Defining user roles)
- Manually sharing Finder content

Related references

- Local and shared content
- Nextthink Library

Manually sharing Finder content

Overview

The Finder is able to export content either to the clipboard or to a file in XML format, regardless of the content being local to an Engine or centralized. The XML can be later imported into another system, again with the help of the Finder.

We exclude from this discussion the content that is local to the Finder itself (sessions and custom actions) or non-sharable (tags). See the reference article on local and shared content content for more information.

Exporting content

To share an item, such as an investigation:

1. Log in to the Finder.
2. Locate the investigation on the left-hand side accordion panel of the Finder.
3. Right-click the name of the investigation and select **Export**:

- ◆ Click **Investigation to clipboard** to copy the contents of the investigation to the clipboard.
- ◆ Click **Investigation to file...** to save the contents of the investigation to an XML file.

If you have organized your investigations in folders, right-click the name of a folder and select **Export** to actually export all the investigations in the folder. To export all the investigations that are visible from the Finder at once, right-click the header of the section **Investigations** (or in the empty area within the section) and select the **Export** option. Again, when exporting multiple investigations, choose whether you want to export the **Investigations to clipboard** or the **Investigations to file....**

Importing content

To import the previously exported investigation into another Engine:

1. Open a Finder session in the other Engine.
2. Right-click the header of the **Investigations** section or in the empty area of the section and select **Import** from the menu.
3. Depending on how you exported the investigations:
 - ◆ Select **Investigation from clipboard**, if you copied the contents of the investigation to the clipboard.
 - ◆ Select **Investigation from file...**, if you saved the contents of the investigation to an XML file.

If any of the imported investigation already exists in the destination Engine, the Finder displays a dialog for resolving the conflicts.

Other sharable content

The method described above using investigations as an example works with other types of content as well. Apply the same method to export and import:

- Investigations
- Investigation-based alerts
- One-click investigations
- Web API investigations
- Categories
- Metrics
- Services

Note that you can manually export and import not only content that is local to an Engine, but also centralized content. Although centralized content is shared by definition, its sharing capabilities are limited to the set of Engines managed by one Portal. Therefore, you may still want to export centralized content to Engines managed by different Portals. For example, this is specially useful for bringing content from a pre-production environment to a production environment.

Related tasks

- Conflict resolution

Related references

- Local and shared content

Importing a content pack

Importing a pack from the Library

To import a content pack from the Nextthink Library:

1. Log in to the Finder.
2. In the left-hand side accordion, select **Nextthink Library**
3. Look for the pack that you want to import:
 - ◆ In the **Browse** tab, look for the pack in a list that you can refine by type of solution and sort using different criteria.
 - ◆ In the **Search** tab, type in some keywords to find the appropriate pack.
4. Click the plus icon to the right of the name of the pack to import it.
5. Resolve conflicts, if any.

Importing a pack from a file

To import a content pack from a file:

1. Log in to the Finder.
2. Click the sprocket icon in the top right corner of the Finder window.
3. Select **Import content pack from file...** from the menu.
4. Choose the content pack file.
5. Review the content to be imported. Each item is imported into an appropriate place depending on its type:

- ◆ Centralized content (categories, metrics, and services) are shared among Engines in the same setup.
 - ◆ Alerts are locally imported into the **global alerts** section.
 - ◆ Investigations and one-clicks are locally imported into their corresponding sections.
 - ◆ Portal modules are imported into your **PERSONAL** section in the Portal.
6. Resolve conflicts, if any.
 7. When the message **Pack <name> successfully imported** shows up, click **OK** to finish the import process.

Sharing the imported modules

When importing a content pack, note that the imported Portal modules stay in your **PERSONAL** section of the Portal. Remember to publish these modules if you want to share them with the rest of users.

Related tasks

- Conflict resolution
- Reusing dashboard content

Related references

- Local and shared content

Conflict resolution

Overview

When importing content, either manually, from the Library, or from a content pack, it is possible that the content to be imported conflicts with content that is already present in the target setup. Investigations, alerts, modules, etc. with the same name as those found among the imported items may already exist in the same locations where the items are copied. Learn here how to deal with these conflicts and resolve them.

Options for resolving conflicts

The resolution of conflicts is a step in the import process, regardless of the method used for importing content. A dialog displays a list of the offending items

along with a choice of possible correction actions to remediate the different issues.

The options available for resolving conflicts depend on the type of content to be imported. The default option proposed by the system to resolve a conflict follows this conservative rule:

- Existing content must not be broken.

See below the list of all possible actions with an explanation of their meaning. Keep in mind that not all of the options are eligible for any kind of item to be imported and that they may have different effects on different kinds of items:

Skip

The item will not be imported.

Replace

The item to be imported takes the place of the conflicting existing item.

Import a copy and Keep both

Both options keep a copy of both the existing item and the item to be imported by automatically renaming this latter, adding a numerical index to its name. The system displays one option or the other for selection depending on whether renaming the item to be imported may break dependencies or not.

Merge

The item to be imported is combined with the existing item to produce an item that is a mixture of both.

Conflicts in metrics

While all other items are identified solely by their name, metrics can also be identified by their *unique identifier* (UID). Although not visible to the user, the system can verify the UIDs of two conflicting metrics that have the same name to determine if they are different versions of the same original metric (same UIDs) or if they are actually two completely different metrics that happen to have the same name (different UIDs).

The options for resolving conflicts between metrics are different when they have the same UID and when they have distinct UIDs.

Choosing the appropriate option

Skip

When the system detects that the item to be imported has exactly the same definition as the existing item with which it is in conflict, it automatically skips the import, notifying the user by displaying the action **Skip (identical)** in the list of conflicting items.

For the cases when the content is not identical, choose **Skip** if you want to preserve the definition of the existing item.

Replace

Replacing the definition of an existing item by that of an imported item has consequences that depend on the type of item imported:

Metrics

Replacing a metric clears the history of the metric in the Portal only if its new definition introduces major changes (for instance, it has different grouping options). You can only replace a metric by another when both have the same UID.

Services

Replacing a service resets its corresponding Service View in the Finder and its previously computed baselines. Nevertheless, the history of the service is preserved in the Portal.

Categories

Replacing a category triggers an automatic retagging of objects when the auto-tagging rules change. In addition, all manual tags are lost.

Import a copy and Keep both

When keeping a copy of both the existing item and the imported item, the latter is renamed with an index. For instance, if you have an item called **Compliance** and you import another item with the same name (therefore causing a conflict with the existing item), the system assigns it the name **Compliance (2)** to indicate that it is a different version of the item.

There are two formulations for this option depending on the type of the items to be imported. The system suggests either one of:

Import a copy, for categories and services

Since conditions in investigations and metrics may depend on the names of categories and services, renaming the imported categories and services may result in broken conditions.

Keep both, for investigations, folders of investigations, alerts, one-clicks, metrics with different UIDs, and modules

The system proposes this formulation for all other types of items that may be renamed safely. The case of modules is special in the sense that keeping both the existing and the imported modules is the only available action for resolving the conflict; therefore, the system automatically takes this action without prompting the user.

Merge

Two types of items may merge with others of their kind:

- Folders (of investigations, alerts, or one-clicks)
- Categories

When folders are merged, the resulting folder combines the contents of the existing and the imported folders. If individual items inside the folder conflict, you must resolve those conflicts separately.

When merging two categories, all the keywords that are present in the category to be imported and not in the existing category are added to the resulting category. The result of the merge, understood as a set operation, is thus the union of the keywords in the two categories.

To determine what to do with the keywords that are present both in the category to be imported and in the existing category, but defining different auto-tagging rules, the merge operation comes in two flavors:

Merge - preserving auto-tagging rules

To preserve the auto-tagging rules of the keyword in the existing category against the auto-tagging rules defined by the keyword to be imported.

Merge - replacing auto-tagging rules

To substitute the auto-tagging rules of the keyword in the existing category for the auto-tagging rules of the keyword to be imported.

For categories, it is recommended to choose first **Import a copy** before committing on a **Merge**. Decide later whether you really want to merge the two categories. If so, re-import and choose **Merge**. After merging, check the order of the keywords in the resulting category.

Conflict resolution table

Find below a table with all the types of objects and the available conflict resolution options for each one of them:

Items	Conflict	Skip	Replace	Import a copy	Keep both	Merge	Merge - preserving auto-tagging rules	Merge - replacing auto-tagging rules
Investigations / alerts / one-clicks	Same name (in same folder)	X			Default			
Folder of investigations / alerts / one-clicks	Same name (in same folder)	X	X		Default	X		
Metrics	Same name (globally) and same UID	Default	X					
	Same name (globally) and same UID				Default			
Services	Same name (globally)	Default	X	X				
Categories	Same name (globally)	X	X	X			Default	X
Modules	Same name (in PERSONAL section)				Default			

Exporting a content pack

Overview

In a previous article, we have already seen how to manually share content generated in the Finder. To complete the picture, learn here how to manually export content from the Portal and, optionally, how to create a content pack for combining both Finder and Portal content into a single file.

The operations described in this article should only be performed by a Nextthink Engineer or a Nextthink Certified Partner.

If you need help or assistance, please contact your Nextthink Certified Partner.

Exporting modules from the Portal

There is currently no graphical interface to exporting modules from the Portal; therefore you need to use the command line. The export process takes the specified module and produces an XML file as output. This file can later be imported into another setup from the Finder in the same way as you would import any other content pack. Note that the tool only lists and exports published modules by default.

To export a published module:

1. Log in to the CLI of the appliance hosting the Portal.
2. Go to the directory holding the export script:

```
cd /var/nexthink/portal/rsquery
```
3. Optional: Display the usage of the export script:

```
./exportLibraryV6.py --help
```
4. Optional: List all the published modules available for export:

```
./exportLibraryV6.py --list
```
5. Export a module to an XML file:

```
./exportLibraryV6.py --export --moduleName="name" \  
--exportfilename="/tmp/module.xml"
```

You can export more than one module at a time by specifying several modules by their name or their UIDs in the export command.

Creating a single content pack file

With the methods for exporting modules from the Portal and other content from the Finder, you have now at your disposal the tools to export any kind of content from one setup to another. However, for your convenience, you may want to put all the content that you want to export from both the Portal and the Finder in a single content pack file.

To that end, edit your own content pack XML file and add all the content to it. If you want to include Portal modules, it is recommended to reuse the XML file generated by the Portal as a starting point to build your own content pack. In any case, the XML of a content pack has the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>  
<Pack Description="brief description" Name="name" SyntaxVersion="1">  
  <Contents>  
    <Content Type="type of content">
```



```
</Content>
...
</Contents>
</Pack>
```

Inside each **Content** tag, copy the Finder or Portal content that you have previously exported as XML files, after removing their own XML header. In the case of Finder content, the XML must contain a tree of objects and not a single object. To export a tree of objects from the Finder, group the content in a folder and export the folder. Alternatively, export a tree of objects by exporting a whole section: right-click the header of a section in the accordion and select **Export**. For instance, to export all your categories at once from the Finder, right-click the header of the **Categories** section in the left-hand side accordion and select **Export**.

Indicate the type of content that you have copied inside the **Content** tag by setting the value of the **Type** attribute. See below the list of all possible values for the **Type** attribute:

PortalModuleCollection

Indicates that the content are modules exported from the Portal.

investigations-tree

Indicates that the content is a set of investigations.

services-tree

Indicates that the content is a set of services.

metrics-tree

Indicates that the content is a set of metrics.

fields-tree

Indicates that the content is a set of categories.

ObjectOneClicksTree

Replace *Object* by the actual name of an object to indicate that the content is a set of one-clicks relative to that object. *Object* may be one of User, Device, Package, Application, Executable, Binary, Port, Destination, Domain, Printer, Execution, Connection, or Web_request.

Note that the **Settings** section in the accordion of the Finder is special when exporting content, because it exports only the content that it is displaying at the moment, be it alerts, one-clicks, or Web API investigations. Note also that the import of Web API investigations via a content pack is not supported. Do not include Web API investigations in your content packs.

One-clicks in particular are also special on their own. When exporting all the one-clicks at once and not only the one-clicks associated to one kind of object, the Finder actually generates a content pack (not a simple tree) which itself includes all the trees of one-clicks associated to each kind of object. Keep this in mind when editing your own content pack.

Related tasks

- Manually sharing Finder content
- Importing a content pack