Nexthink V6.24

Library Packs Configuration

Generated: 4/07/2021 1:21 pm

Copyright Nexthink, Inc. All Rights Reserved

Table of Contents

Configuration Manuals **1**
- Overview 1
- Installing a New Version of a Library Pack 1

Device management **4**
- Reduce logon duration 4
- Group Policy Management 4
- Hardware Asset Renewal 5
- Overview 5
- Hardware Asset Renewal 5
- Hardware Asset Renewal Advanced 6
- Application Auto-Start Impact 8

Remote Employee Experience **10**
- Remote Worker Experience 10
- Home Networking 16
- Home Networking 29
- Change Log and Upgrade process 43
- Remote Worker vs Office Worker Device Category 48
- Remote Worker Insights 49

Compliance **51**
- Device Compliance 51

GSuite **54**
- GSuite: Health 54
- GSuite: Services 54
- GSuite: Sentiment 55
- GSuite: Advanced health 56
- GSuite: Advanced Health 56

Support **58**
- Support: Level 1 58

Shadow IT **59**
- Shadow IT 59

Table of Contents

Malware Protection **61**
Malware Protection 61

Office 365 Health **63**
Office 365 Health: Overview 63
Office 365 Health: Overview 63
Office 365 Health: Services 63

Office 365 OneDrive **65**
OneDrive Summary 65
OneDrive Operations 65
OneDrive Advanced Health 67
OneDrive Migration 67
OneDrive Sentiment 70
OneDrive Management 70

Office 365 Teams **72**
Teams Overall Configuration 72
Teams - Migration 74
Teams - Health 76
Teams - Advanced health 78
Teams - Adoption 81

Office 365 ProPlus **98**
Office 365 ProPlus - Operate 98

Virtualization **101**
Virtualization: Health 101
Virtualization: Operate 101
Virtualization: Citrix Advanced 103
Virtualization Planning and Migration 105

Windows **106**
Win10: Configuration 106
Win10: Migration 106
Win10: Feature Update 108
Win10: Quality Update 108
Windows Defender Management 109
Administrators Management 110

Table of Contents

Webex **113**
Webex Operate 113

Zoom **115**
Zoom Operate 115

Remote Actions **116**
Get Performance Monitor Data 116
Restart Device 117

Configuration Manuals

Overview

Find here the configuration manuals of the packs in the Nexthink Library that require nontrivial steps to get them up and running.

The configuration manuals of the different library packs are available in this same **Library Packs Configuration** section, starting from the minimum version of the product that is compatible with each pack.

Related references

- Nexthink Library

Installing a New Version of a Library Pack

When a Library Pack is updated with more features and bug fixes, the initial release (e.g. 1.X) is superseded by the new (e.g. V2.X). This is indicated in the first Portal dashboard in the pack, where in the slide-out help on the right you will see the current version of the pack you are using:

Use this method to understand which version of the pack you are using.

Installing a Clean Copy of a library pack

If you are in fact not upgrading, but installing the new Library Pack for the first time, simply download it from the Nexthink Library and select Install, all new content will be installed in the various areas of the Finder and Portal. The

"Conflict" dialog could be displayed as there may be Categories shared with another pack. Refer to the Conflict Resolution documentation for further help.

Upgrading to the latest version of an existing library pack

If you have a Library Pack installed and are looking to install the next version of it, there are two possible ways.

Removing the existing library pack and install the new version

The first, which is the most straightforward, is to fully remove the existing library pack (Dashboards, Metrics, Investigations, Categories, Campaigns, Services) and then do a clean install of the new one. In this scenario be aware you will lose any customization. In particular keep in mind the configuration you might have put into Categories and Metrics. You will also lose historical data in the Portal for this pack as you are doing a complete remove / replace. If this is not of critical importance to you, then proceed in this fashion.

Post removal, you would proceed as normal with the pack installation and configuration.

Migrating from a version to the next

Should you wish to upgrade from a version to the next without removing the existing library pack, it is a slightly more involved process. The advantage of this method is you will retain your historical data in the Portal.

When doing an import with the library pack already present, a number of items may report conflict in Finder. Please see the Conflict Resolution documentation for instructions on how to manage the conflict resolution process.

Should you be upgrading, as per normal Nexthink behavior, the Portal will install new dashboards with a numerical denominator next to them to indicate they are the new ones. Align any dashboard customization's as you wish using normal

Portal editing options such as copying and pasting widgets and dashboards and then remove the extra dashboard copies you no longer need.

Device management

Reduce logon duration

You can adjust the threshold of the logon and extended logon duration to your need. By default, thresholds are the same than used in the DEX score.

To change thresholds, modify the following 2 metrics:

1. **Reduce logon duration- Devices with poor logon duration**
2. **Reduce logon duration- Devices with poor extended logon duration**

Group Policy Management

To use this library pack the following remote action need to be be executed on all devices.

Remote Action: Get Gpo Startup Impact

This Remote Action is found within the Nexthink Library > On Demand area:

Recommendation is to run this remote action every week. It is possible to use this investigation to execute it on all Windows workstations: **Group Policy Management - All Windows computers**

Hardware Asset Renewal

Overview

The Hardware asset renewal pack helps you manage the life-cycle of your devices. It is based on the Digital experience (DEX) device score which measures the actual experience with your devices. The Hardware asset renewal dashboards give you an idea of the physical devices that you need to replace, rebuild, or keep.

Hardware Asset Renewal

Hardware asset renewal costs score

The costs for replacing, rebuilding, or upgrading a device must be configured inside the **Hardware asset renewal costs** score. Once the values have been adapted to your situation, You should update the **Hardware asset renewal** score. The default values for the **Hardware asset renewal costs** are listed below:

◊ Replace (500 $)
◊ Rebuild (200 $)
◊ Upgrade disk (100 $)
◊ Upgrade memory (100 $)

Categories

- **Hardware type** - The keywords in this category are used to define the model and type of hardware that you are looking to evaluate.

- **Hardware assessment** - The Evaluate keyword in this category is used to define the operating system and device type of the machines you are looking to evaluate.

Hardware Asset Renewal Advanced

The Hardware asset renewal advanced pack helps you manage the life cycle of your devices. It is based on the Digital Experience (DEX) device score which measures the actual experience with your devices along with the hardware asset health score next to it.

Prerequisites

This pack uses the same categories as the Hardware Asset Renewal library pack. Descriptions for these categories can be found here. Ensure they are custom configured to your environment.

Remote Action Configuration

- **Get Warranty Information** - Remote Action must be executed against your devices to obtain the warranty information of the Dell and Lenovo devices present in your environment. In the Parameters, enter the details of the relevant devices for the Dell Lenovo devices in your environment.

- **Get Disk Health** - This Remote Action must be executed against your devices to obtain the disk health information. Simply input the target drive letter in the Parameters section and the minimum threshold for disk temperature.

- **Get Battery Status** - This Remote Action returns the health status of a laptop battery. It requires no arguments, simply run it against the target machine(s).

- **Get Boot Details** - This Remote Action returns information regarding a Windows machine boot details. It requires no arguments, simply run it against the target Windows machine(s).

- **Set Boot Autologger** - This Remote Action Enables or disables an Autologger configuration on Windows 10 and 7 machines so that you can create a boot trace. In the Parameter section, simply enter one of the following string values "enable" or "disable" depending on your goals. In the Campaignid section, simply input the id of the campaign associated with this Remote Action. If no campaign is associated with it, you can leave it blank.

Hardware asset renewal costs score

Each action should be associated with a cost. The costs can be defined in the **Hardware asset renewal costs** score. By default, the costs are as follows:

- ◊ Replace (500 $)
- ◊ Rebuild (400$)
- ◊ Upgrade disk (100$)
- ◊ Upgrade memory (100 $)
- ◊ Change battery (100 $)

After making these changes, you should also update the **Hardware asset renewal savings** score as well.

Application Auto-Start Impact

To use this library pack the following remote actions need to be be executed on all devices.

Remote Action: Get Startup Impact

This Remote Action collect application startup impact measured by Windows 10. Can be found within the Nexthink Library > On Demand area:

Recommendation is to run this remote action every week because startup impact is evaluated by operating system after a complete boot.

The following investigation is ready to use to execute the Remote Action on all Windows 10 workstations: **Application Auto-Start Impact - All Windows 10 computers**

Remote Action: Disable application from Startup menu

This Remote Action allow to disable a list of application or all application not listed in the white list. Can be found within the Nexthink Library > Remediation area:

Application to disable or keep can be copied from **Applications output** of **Get Startup Impact** Remote Action.

Recommendation is to run this remote action every day.

Remote Employee Experience

Remote Worker Experience

Overview

The Remote Working Experience Pack enables you to manage the experience of your remote workforce. Whether working remotely out of choice or necessity, the digital experience of the remote worker is vital as their isolation makes them completely dependent on their digital devices.

The pack has a number of dashboards, categories, metrics, and campaigns but note that these are an out-of-the-box configuration and customers are absolutely free to configure the pack as they wish, details of how to do this are in this article.

The pack gives you a readiness-assessment of your infrastructure to ensure that your employees are able to successfully stay productive and collaborate with their colleagues, whether remotely or in the office. The pack covers a number of aspects, such as software presence, encryption status, and whether a VPN authentication certificate is present.

The pack will allow IT teams to monitor, manage, and report on their employees' digital experience and by taking both technical and sentiment metrics into account, it will provide complete employee-centric infrastructure visibility. It monitors the usage of the remote connection so that the network traffic can be optimized and forewarns of impending user experience issues such as passwords soon to expire.

In particular, the pack focuses on the device readiness and configuration and the success of Microsoft Teams, Skype for Business, and Zoom. (If your organization does not use these tools, then the appropriate dashboards and metrics can be removed).

The pack comes with Sentiment campaigns for both IT Topics, such as Service Outage and IT Satisfaction along with HR-centric campaigns on items such as Employee Well-being.

You can also detect the Wi-Fi signal strength for the remote devices and a self-help campaign can assist the employee in getting better Wi-Fi reception.

There is a dashboard on the compliance of your remote Office 365 ProPlus devices. This is particularly useful in the concept of Remote Working because patching and staying up to date is more complex when you are outside the Office networks so we have taken the key parts of the Office 365 ProPlus pack and added it into Remote Worker, but keeping the focus on your remote workforce.

Platforms Supported

- macOS
- Windows

Additional optional library packs

There are additional packs on the Nexthink Web Library that can be used in addition to the Remote Worker Experience Pack to enhance the view of Remote Workers even more:

1. L1 and L1 Advanced Checklists ? these have been updated to include various checks pertinent to remote workers such as VPN and Firewall being present, collaboration tools being installed, the Wifi signal strength, and key items such as impending password expiration which can have an increased impact on remote workers due to their distant proximity to physical support staff.
2. Windows Defender Management ? This pack now includes greater detail and a breakdown of its metrics for Remote workers versus Office workers.
3. Device Compliance - this pack has been upgraded in two aspects. Firstly, the Remote Worker view has been added as a breakdown so that on all dashboards a breakdown is given by worker type to help you understand where your workers are in the context of each dashboard. Secondly, there is a significant update to the Software Compliance dashboards which allow you to configure any piece of software at any version level and Nexthink will report your corporate compliance level in regards to it.

If you wish to download or upgrade to the latest version of the above packs, feel free to do this outside the activities below which are covering the core Remote Worker pack configuration.

Pre-Requisites

The Remote Worker Experience pack refers to Digital Experience Scores in some of its dashboards, therefore the Digital Experience Score pack should be installed before installing the Remote Worker Experience pack. This pack is

macOS enabled so if you want to target macOS machines you must ensure that the Digital Experience Score for macOS pack and macOS Content Pack have been installed as they are needed for macOS compatibility.

Change log & Upgrade Process

If you are upgrading from an earlier version of a library pack follow this link to read about the upgrade process from a version of a Library Pack to the next one.

Follow this link to read about the Change log of the Remote Worker library pack.

Configuration

The pack requires some level of configuration so that it can correctly identify remote workers. These configuration steps should be set to the values relevant to your organization before using the pack so that the results are accurate.

Because of the multiple possibilities in the configuration of Remote Workers, it is also possible to amend metrics, this will also be covered.

User category "Remote Worker vs Office Worker"

Use this category if you wish to identify users as remote workers by assigning this manual category. To use, simply create an investigation of all users you wish to categorize as remote and set the keyword so that they are categorized as the "Remotely Connected Worker".

Device category "Remote Worker vs Office Worker Device"

This category is used by multiple library packs. Please go to its dedicated configuration page for more information about it.

Device category "Remote Worker Readiness"

This category should be configured to describe the types of devices that remote workers will be using, using whatever criteria you wish. During the execution of the pack, in the readiness assessment dashboards, these criteria are used so that only the readiness of devices that match the criteria wished are reported on. For example, should you just use laptops for remote workers, then the "Remote Worker Devices Type" tag within the category can be set to just laptop. Likewise, if you are using Desktops and Laptops in the office, then "Office Worker Devices Type" can be set to Laptop or Desktop. It is entirely possible to have more than one entry for each tag should you use laptops, desktops, virtual desktops, or

other configurations for your workforce.

Package categories "Firewall / AV / Other Packages" and "VPN Packages"

These three categories define packages that you wish to look for in the pack. The Packages should be present on a remote working before it is considered compliant and ready for remote working. It is entirely possible to customize these entries to match the requirements of your organization, the default values hold commonly used applications.

Executable categories "Firewall / AV / Other Executables" and "VPN Executables"

These three categories hold the equivalent executables for the earlier Package based categories. This is needed because although we can look for installations with categories if we wish to list version dispersions and so forth we need to go to the executable level. Once again, full customization is possible, change the entries as you wish to match any particular executables you wish to track.

Domain category "Unwanted Domains"

This optional category holds any domain or domain category that you either simply want to track or do not want users to be using. The associated metrics do not stop users visiting these domains, Nexthink cannot do this. However, it reports on the data volumes going to them.

Package categories "ProPlus Required Version" and "ProPlus Version"

The Remote Worker pack provides a dashboard showing you the key information regarding Office 365 ProPlus. This information is largely taken from Nexthink's Office 365 ProPlus - Operate pack and these Categories, while included in the Remote Worker pack, are simply references to the categories found in the ProPlus pack - therefore if you have already imported the ProPlus pack, no configuration is necessary. If you have not imported the ProPlus pack and would like to see the core information around patching and DEX when it comes to Office 365 ProPlus for your remote workforce, then these two categories should be configured.

- "ProPlus Required Version" - The dashboard is entirely flexible in terms of what versions of ProPlus you wish to monitor. By configuring this Category you are describing which version(s) of ProPlus you wish to monitor. This category should contain the version number(s) you would like to achieve across your remote ProPlus landscape. Note that any version number can

be added and multiple versions can be used (for different ProPlus branches). Details on ProPlus version history is published by Microsoft.
- ProPlus Version - this should contain all the versions of ProPlus which you currently support within your Organization, configured in the same way as the above-Required Version Category.

Destination category "Update Servers"

The Windows 10 portion of Remote Worker Experience has indicators as to whether devices have received traffic from update servers, which can reveal any change in Digital Experience soon after updates are received.

To support this, the "Update Servers" category has been created, which should be populated with the names of your update servers, normally SCCM Distribution Points within your environment.

Campaigns

The pack also contains five Campaigns, which can be used as wished.

Satisfaction Campaign

This Campaign is intended for continuous feedback on Remote Working experience. Examine the Campaign details in terms of the title and description amending as wished. When ready, publish the Campaign. It is targeted at the Investigation "Remote Worker Experience - Users working from home" so when published this Investigation will be evaluated and continue to be so every 10 minutes following. The Campaign is configured so that recipients will get the Campaign once every month.

Information Campaign

This Campaign is intended to update remote workers (or any targeted users) with informational updates of any sort. This could be a news update regarding a hot topic within the company, a reminder on some best practices, it really is anything you wish to put into it. When ready, publish the Campaign. It is targeted at the Investigation "Remote Worker Experience - Safety measures audience" so when published this Investigation will be evaluated and continue to be so every 10 minutes following.

Service Outage

This campaign is particularly aimed at quickly informing people of service outages or degradations. When connected remotely it can be frustrating if services go offline, so this campaign allows the quick delivery of service status messages. The pack includes a campaign targeted for Microsoft Teams. However, this can be modified to cover any service name.

Well-being Campaign

This Campaign is aimed at the well-being of employees from a non-IT perspective. While working remotely it is important not just to track the technical side of the employee experience but also their overall happiness and satisfaction with their remote working experience. The campaign is targeted at Remote Workers by default.

Get Wi-Fi Signal Strength

This Campaign is launched when the Remote Action "Get Wifi Signal Strength" is launched against a remote device. The WiFi network at the remote destination is measured and should it be below a certain threshold (one of the input parameters) then it will launch this Campaign, which is self-help for the user. We encourage you to modify the Campaign with any self-help tips that you would like to bring in for your Organization. The Campaign also asks the User whether the tips were useful so it brings an understanding as to whether the tips being offered are of use.

Metric Modification

The metrics to track software installation and uninstallation use a particular mechanism. Within the Readiness assessment branch of the metrics, you will see that the criteria are looking for the presence of either a single package or multiple packages. If it's a single package, you can simply change the package name in the relevant category and the metric will look for the new name. if you wish to add more criteria, for example, say you wish to look for the presence of five packages, the key is to add the additional criteria using the existing logic of "Package...<Category>...is...<Item>" but note that in the "and" section further down, the total number of packages you are looking for should be incremented: If you are looking for five packages, this should be updated to five and so on.

Customers are actively encouraged to tune the metrics testing if the certificate pair is valid. For example, removing the Private certificate check if that is not relevant to their setup.

This ultimately means full flexibility: for any of the categories in the pack you can have as many packages or executables you want and you can amend the metric criteria accordingly if you wish to search for more packages or executables being present before considering the device compliant.

Home Networking

Introduction

The Home Networking pack measures the employee Digital Experience from home providing insight using both the existing Digital Experience Scores that is part of Nexthink's core technology, through to the actual health and speed of the connection. It is built around Remote Action output as well as core Digital Experience metrics and as such, some configuration is necessary for the pack to function correctly.

With the pack in place, we can measure the health of the local connection of the device, the speed and Round Trip Time (RTT) to external and internal websites, and file shares. Any of the components can be enabled or disabled as desired.

Pre-Requisites

Before implementing the pack it is important to fully understand the remote network connection mechanism for the devices (more details below).

Also, the Digital Experience score library pack should be fully installed in your environment as these values are used in the metrics configuration.

Because the dashboards use the Digital Experience score version 2.x it is required that version 6.27 of Nexthink is installed, the recommended being 6.28 or above.

Overview of Client Configuration and Split Tunneling

Affecting all the Remote Actions in this pack is a need for a clear understanding of device configuration. Consider a typical setup that might be found in a customer environment:

This kind of configuration, with different routes possible to different services, must be understood for the Home Networking pack to be effective. Note that it's entirely possible instead to have a simple configuration ? if all traffic goes down a VPN, or if all traffic goes out to the open Internet with no other alternative possible, then the configuration of the Remote Actions will become simpler. Commonly, in larger environments, to separate the traffic, some will go directly out to the open internet, some going to SaaS services through an IP Tunnel and some might go down a VPN to the datacenter. When configuring the Remote Actions in the pack, always understand what route will be taken by the traffic going to a particular destination as it affects the results you are getting back:

- ◊ If you wish to measure the download speed of the pure internet connection, for example, then ensure the file that you place in your cloud service is accessed via the local internet facing interface and not via a VPN interface if one exists ? because if it goes down the VPN, you?ll end up with the download speed of the company internet connection as the packet will be going through the VPN, through the company network, and out their internet connection.
- ◊ The same principle applies for all configurations ? for the RTT to websites, if what is wanted is the RTT via the home direct connection to the internet, then make sure that the destinations to those websites are not going down the VPN connection because if they do, then, in fact, you will measure the speed down the VPN, into the corporate network, out the corporate network?s internet connection, to the website and then back again.
- ◊ There may well be cases, such as the download speed to the UNC location where you do want it to go correctly through the VPN to the company and back. In this case, make sure that the configuration on the device is such that this traffic goes out through the VPN

interface.

- ◊ Also - and separate to the individual Home Networking Pack - if you choose to use the Geolocation RA which can be downloaded from the Nexthink Library, consider this too ? the Geolocation RA uses a third-party service, ipapi.com for its lookup. In this instance, make sure this domain (fully) is not going down your VPN - otherwise, you will end up with the ISP of your Corporate provider and not the local connection.

Home Networking Remote Actions ? Configuration

The Home Networking Library Pack uses a number of remote actions. This page outlines how to configure these for optimal use. The following RA?s are involved in the solution:

Get Local Speed to Gateway

Get Local Speed to Gateway ? determines various connection health and speed properties of the local connection into the home router/default gateway. This doesn?t need any additional parameters to be configured as it is a simple test to the local router, however, we recommend leaving the randomized delay in at the start the default of 60 seconds so that not all clients execute this at the same time.

The one input parameter, **MaximumDelayInSeconds** is the Maximum random delay set to avoid network overload. This defaults at 60 seconds and we recommend leaving at this value as this test is only to the local gateway of the employee, it does not impact the corporate network.

Get Network Speed

This Remote Action will determine the speed, in terms of the Round Trip Time, to a given URL and report this back. It also gives Boolean outputs for whether this is greater than the threshold that is requested enabling dashboarding of this property.

Two input parameters define whether this is a public URL or a Business URL. In fact, these are interchangeable, they are just functional guidance, i.e. you can leave two external sites, two sites that are internal to your network, it's entirely flexible, they are just two URLs. The Remote action will test the round trip time to these two URL?s and report them.

The configuration required is simply to ensure that the URL?s are configured and once again think closely about what is being tested ? if the test goes down the VPN to the URL then it's not a test of the internet latency direct from the home network, it?s a test of the latency to that URL which (if this is the intended configuration) may well be a web service in a data center. If it goes to a public URL such as google it is more a test of the response time of their device to the internet. A threshold defines the level at which the RTT is considered too slow and marked as bad for that test run.

When public Round Trip time is higher than the average set in the threshold it is a sign of a bad connection. We recommend executing the Remote Action frequently because connection quality can change during the day. Note that you do not have to give both parameters, you can configure one only if wished.

IMPORTANT: From a dashboarding perspective from this pack, this RA also returns the value ?Connection Type? which is used in a lot of the dashboarding, so it is important that this RA is running at least daily to keep the dashboard reflecting the correct data for all RA?s in the pack. Ideally, as this is low bandwidth, it should be run more frequently (hourly). Note that the Connection Type property can be Wired, WiFi, Cellular, or ?Unknown?. This last type may be encountered in certain VPN configurations where Nexthink cannot retrieve the VPN configuration with guaranteed certainty, so shows Unknown in this instance as a reflection that we cannot guarantee what we have found.

There are some parameters to note:

- **MaximumDelayInSeconds**: Maximum random delay set to avoid network overload. Provide the number of seconds lower than 600, Nexthink recommends setting this between 60-300 seconds to balance getting prompt results with overloading the environment with multiple devices querying the destination at once.
- **ExternalURL**: The external URL to check the Web RTT against.
- **WebRTTThreshold**: The time threshold for the external URL Web RTT. Nexthink can recommend a value here, such as 600ms, however, it is going to be very specific to the customer environment. We recommend setting this according to your needs after running it with the default parameter of 600ms and seeing which values are coming back from your devices. Note that there is a dashboard metric, ?Home Networking - Internet Connectivity - Devices with high RTT to external URL? which also uses this threshold in its calculation so if the value is changed in the RA, please update the metric accordingly. This also applies to the equivalent metric which covers the Business URL.

- ◊ **BusinessURL**: The URL in the corporate environment to be checked the Web RTT against
- ◊ **BusinessWebRTTThreshold**: The time threshold for the business URL Web RTT, please see above for ?WebRTTThreshold? for guidance on this parameter.

Get Download Speed

The Get Download Speed Remote Action downloads a file placed on a cloud service or a file share and will then calculate the speed of the connection based on the time taken to download this file. Please note the file is not fully downloaded to disk, it is simply streamed to the local device and the calculation made.

It will use whichever interface is configured for this destination. Note that with the possibility of UNC and URL based locations that can be specified, ensure that you understand the configuration needed on the client to make sure you go in the right direction for each download.

VERY IMPORTANT:: This Remote Action downloads a file. There is a randomized delay as per normal that can be set up to 600 seconds however if run across a wide range of devices be absolutely sure that you understand what is happening. It is the intended behavior but particularly for files placed on UNC locations consider that many machines may download this at the same time. It is why we recommend a 50-100mb file as the optimal size if network capacity allows it.

There are three parameters to understand:

- ◊ MaximumDelayInSeconds: Maximum random delay set to avoid network overload. Provide the number of seconds lower than 600. This parameter should be left high because this Remote Action can absorb significant network traffic, so having all devices execute at the same time is not desirable. We recommend leaving this at the maximum, 600, which will mean it may be up to 10 minutes before the Remote Action completes.
- ◊ BusinessServiceUNC: Path to a file located in a corporate network's shared location. Eg. \\server\\SharedFolder\\file.txt.

IMPORTANT - Do not use a large file or this could flood your network. Provide an empty value to skip this test. Nexthink recommends a value of between 50-100mb for optimal results of this Remote Action if your corporate network will allow it.

- ◊ BusinessServiceURL: URL to a file located on a cloud location which will then be downloaded to perform the speed test. IMPORTANT - Do not use a large file or this could flood your network. Provide an empty value to skip this test. Nexthink recommends a value of between 50-100mb for optimal results of this Remote Action if your corporate network will allow it.

The following steps now go into how to configure the files which will be downloaded in more detail. If you are not planning to use this Remote Action these steps can be skipped.

Get Download Speed Remote Action ? Creating the Test File on the Cloud

The Get Download speed Remote Action downloads a file placed on a cloud service. It will use whichever interface is configured for this destination. Note that with the possibility of UNC and URL based locations that can be specified, ensure that you understand the configuration needed on the client to make sure you go in the right direction for each download.

NOTE: This example uses Azure, however, any cloud storage is possible, for example, AWS. Ensure that the client devices can reach the file destinations, both the UNC and HTTPS (if both are configured) otherwise you will get a failure to connect the message. The Get Download Speed Remote Action has both HTTPS and UNC parameters for both files on the cloud and files on a file share.

Cloud Test File Configuration

To configure this component a file must be placed on a cloud service that can then be downloaded. It should not be too big (we recommend about 50mb) and it is mandatory that it has open access because the mechanism to download the file needs to be unauthenticated. The following steps outline how to achieve this using Azure, though any cloud provider can be used.

1. log into the Azure Portal (this example uses Azure but any cloud provider can be used).
2. In Any Resource group you wish, create (by clicking on the ?+? sign) a new object of type ?Storage Account?:

note the importance of the location field for where it will be based and how it will be accessed (https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy).

3. Set the properties of the storage:

4. Continue the wizard to describe the properties of the storage account in terms of networking, data protection, advanced settings, and tags. This is entirely dependent on your choice as an organization, please consult your Azure, AWS, or other cloud service team if in doubt.
5. Finally click on Create in the Review and Create to create the storage.
6. Go to the storage and go to Storage Explorer (Preview) and select Create File Share. Note that you can also create a Blob Storage to do this also (in this case make sure you enable anonymous access in the wizard).

7. Create a file share with a suitable name for your Remote Action test.
8. Refresh the page and now you are able to upload a file into the share:

9. Upload the file you wish to test from bearing in mind that too small may give inaccurate results, too large will potentially congest your network. This can be as you wish, here at Nexthink we recommend a 50-100MB for the most optimal results. Due to the way the file is streamed to the client (though not actually downloaded) it must be a .bin extension. This does not have to be a real binary file, it can be something harmless like a text file renamed. If you use other file types you may receive an error in terms of MIME type when the remote action executes.
10. Once uploaded refresh the page, the file is now there in the file share. Now right-click on it and choose Get Shared Access Signature and set the length of access to where you desire:

11. Once created now copy this URI

12. Now paste this into the parameter field in the Remote Action for the BusinessServiceURL:

Get Download Speed - UNC Parameter

A UNC parameter can be specified for the DownloadSpeedUNC. In this instance, the configuration is much simpler but again care must be taken. Firstly, if you configure this property make sure that the device can get to the UNC location, if not, the RA will fail. Once you are sure of this, the UNC parameter, in the simple form of \\server\share\filename is specified. The Remote Action runs in the context of the current user, so they must have access to the share. With this configured, the RA will execute successfully. Note that for this Remote Action,

the Maximum Delay in Seconds should be 600 so that there is a randomized start to the activity so as not to flood the network.

Get Wifi Signal Strength

This will check the signal strength of the WiFi connection and report it back. It will also work on a threshold (configurable) of **AcceptableSignalQuality** which indicates the signal strength that must be reached to be considered acceptable as a percentage. If below this signal strength on each execution it is noted by the Remote Action and if the number of times this occurs in 24 hours passes the **AlertUserAfterBadSignals** value then there is a campaign attached to this that informs the user of how to get a better WiFi signal. This campaign is very basic, and the idea is it can be evolved as wished. If your customer wishes to use it, it is a good idea to upgrade it to a relevant set of campaign statements for your environment. We recommend running this Remote Action regularly so that the Wifi signal is tested regularly throughout the day, ideally hourly.

A number of parameters are available for this Remote Action:

Connection

- **CorporateNetworks**: Comma-separated list of SSIDs which are defined as corporate. It can be empty
- **AcceptableSignalQuality**: Minimum signal quality percentage to consider the current wireless network as good (0 to 100), Nexthink recommends a value above 80 here.
- **AlertUserAfterBadSignals**: Number of times (1 to 200) the signal has to be under the acceptable threshold during the current day to notify the user via a campaign. This will depend on how many times you wish to run the Remote action. Nexthink recommends running this hourly, so on a given day there will be 8 samples taken, so if this value is set to 4, then 50% of signals over the course of a day would have to be poor and it would trigger the campaign.

- **CampaignId**: Campaign to show with recommendations such as getting closer to the router. Use an empty GUID (00000000-0000-0000-0000-000000000000) to avoid the campaign.

Get Wifi Signal Strength: Co-Channel interference

If a remote worker is in an environment in which there are multiple networks operating on the same channel, congestion occurs in that channel. This congestion results in slow network speeds and reduced productivity. Below is a diagram of a home networking setup that can cause Co-channel interference:

In the context of home networking, if a remote worker has multiple networks sharing the same channel, this decreases the network throughput and reduces the overall quality of their home networking experience. The following measures can be taken to avoid Co-channel interference:

- To fix the issue the competing access points should be moved to a new channel so they don't interfere. There is a Campaign within the pack that can be sent to the employee advising them how to improve their wifi signal strength, which by default advises them to move closer to the access point. This can be enhanced if there is co-channel interference with some advice to reconfigure one of their access points to point to a new channel. NOTE: The steps to do this will depend on the access point type which may vary per employee."

- If the employee is running a 2.4ghz WiFi network, the campaign can be modified to

advise them to move to 5ghz (if range allows it, as 5Ghz has less range). Likewise, it can be a good idea to modify the strength of the signal if one of them is weak. Note: If the employee's WiFi routers support mesh networking, this should automatically reconfigure the WiFi networks so this issue should not occur. This would be the best solution but may come at a cost for the employee. Additional solutions can be to move the access points further away from each other and to keep a 20 dB received signal strength indication (RSSI) or more between networks on the same channel.

- **Adjacent-Channel interference**

  If a remote worker is in an environment in which there are multiple access points broadcasting on overlapping channels, data corruption, and transmission issues occur. This will result in poor signal quality and subsequently a lower home networking experience. The following measures can be taken to avoid adjacent-channel interference:

  - Move access points further away from each other.
  - Use the 5GHz band to increase the amount of non-overlapping channels to 24. If only the 2.4 GHz band is available, use the non-overlapping 1, 6, and 11 channels.

The parameters that are relevant to cochannel interference are:

- **NearbyNetworksAcceptableSignalQuality** is the minimum signal strength, as a percentage, that a competing network must be at to consider it for analysis as to whether it has an overlapping channel with your current Wifi network. So for example, if you have a Wifi network that has the same channel number as your current one (i.e. will interfere) but you have an acceptable signal quality value of 20% and the competing network is only at 20% then it will not be counted. This is because often in cities there are many low strength networks present.
- **NearbyNetworksMaximumSignalDifference** is the difference in signal strength that must exist for the analysis to complete. For example, if the signal strength of your network is 80% and a competing network is at 20%, but the maximum signal difference is 50% then this will not count because 80-50>20. If the competing network were at 40%, then it would (80-50<40). This factor is used because there must be a significant strength for wireless networks to actually interfere with your signal.

It is recommended that this RA is run regularly, ideally hourly, so that single bad signals do not interfere with the results, i.e. the values are sampled regularly during the day.

Optional - Geolocation RA

This RA is not part of the Home Networking pack but may be used if wished. The purpose is to give more information about where the local connection is originating from. The Geolocation RA has been updated so that it can return more than just the location, it can now return the ISP name which is useful for

customers who want to know which ISP?s are in use.

The RA uses a service from a third party, ipapi.com, who has services ranging from free to paid subscriptions, paid monthly. The use of ipapi.com has been approved by Nexthink Security and Compliance. The free service allows location lookup and up to 10000 executions per month. This has been around for some time at Nexthink as an RA and is still available to use and the Remote Action will still work.

Should you wish to retrieve a greater range of information there are paid subscriptions that can be used. Note that it is customer-centric ? the customer should subscribe themselves to the plan they wish, they will then receive a key that can be used as a parameter in the Remote Action. If a subscription level of ?Standard? or above is chosen then the Remote Action will now return the ISP as part of the returned data, which can be useful for customers who want to look at home networking from this particular angle.

IMPORTANT: An absolutely key point here is that the route to *.ipapi.com should go out of the correct interface in a split tunneling configuration. In the event that the customer uses split tunneling, the traffic must go out of the internet-facing interface and not the VPN interface. If it goes out of the latter you will only get the ISP of the Business as it is really going out of the Business?s gateway. This may well require the addition of this URL to the proxy.pac (or whatever autoconfiguration URL is being used) on the devices that are to run this RA.

- **Get Geolocation** ? Note: Not part of the core Home Networking pack ? is used to give location information on the connection and also optionally ISP details.

    - APIKey: API key to be used for the external geolocation service
    - HTTPS enabled. Valid values are true/false
    - Maximum random delay set to avoid external API overload. Provide the number of seconds lower than 600

Scoring

The pack has a custom Nexthink Score for connectivity (the Connectivity Score). This is a standard Nexthink Score which is targeted at Physical Desktops and Laptops. The score can (and is recommended) to be customized as per the normal Nexthink configuration. An outline of the score is described below, it is taking each Remote Action output and summarizing up into an overall score describing both the local and network connectivity.

Home Networking

Introduction

The Home Networking pack measures the employee Digital Experience from home providing insight using both the existing Digital Experience Scores that is part of Nexthink's core technology, through to the actual health and speed of the connection. It is built around Remote Action output as well as core Digital Experience metrics and as such, some configuration is necessary for the pack to function correctly.

With the pack in place, we can measure the health of the local connection of the device, the speed and Round Trip Time (RTT) to external and internal websites, and file shares. Any of the components can be enabled or disabled as desired.

Pre-Requisites

Before implementing the pack it is important to fully understand the remote network connection mechanism for the devices (more details below).

Also, the Digital Experience score library pack should be fully installed in your environment as these values are used in the metrics configuration.

Because the dashboards use the Digital Experience score version 2.x it is required that version 6.27 of Nexthink is installed, the recommended being 6.28 or above.

Overview of Client Configuration and Split Tunneling

Affecting all the Remote Actions in this pack is a need for a clear understanding of device configuration. Consider a typical setup that might be found in a customer environment:

This kind of configuration, with different routes possible to different services, must be understood for the Home Networking pack to be effective. Note that it's entirely possible instead to have a simple configuration ? if all traffic goes down a VPN, or if all traffic goes out to the open Internet with no other alternative possible, then the configuration of the Remote Actions will become simpler. Commonly, in larger environments, to separate the traffic, some will go directly out to the open internet, some going to SaaS services through an IP Tunnel and some might go down a VPN to the datacenter. When configuring the Remote Actions in the pack, always understand what route will be taken by the traffic going to a particular destination as it affects the results you are getting back:

- ◊ If you wish to measure the download speed of the pure internet connection, for example, then ensure the file that you place in your cloud service is accessed via the local internet facing interface and not via a VPN interface if one exists ? because if it goes down the VPN, you?ll end up with the download speed of the company internet connection as the packet will be going through the VPN, through the company network, and out their internet connection.
- ◊ The same principle applies for all configurations ? for the RTT to websites, if what is wanted is the RTT via the home direct connection to the internet, then make sure that the destinations to those websites are not going down the VPN connection because if they do, then, in fact, you will measure the speed down the VPN,

into the corporate network, out the corporate network?s internet connection, to the website and then back again.

- ◊ There may well be cases, such as the download speed to the UNC location where you do want it to go correctly through the VPN to the company and back. In this case, make sure that the configuration on the device is such that this traffic goes out through the VPN interface.
- ◊ Also - and separate to the individual Home Networking Pack - if you choose to use the Geolocation RA which can be downloaded from the Nexthink Library, consider this too ? the Geolocation RA uses a third-party service, ipapi.com for its lookup. In this instance, make sure this domain (fully) is not going down your VPN - otherwise, you will end up with the ISP of your Corporate provider and not the local connection.

Home Networking Remote Actions ? Configuration

The Home Networking Library Pack uses a number of remote actions. This page outlines how to configure these for optimal use. The following RA?s are involved in the solution:

Get Local Speed to Gateway

Get Local Speed to Gateway ? determines various connection health and speed properties of the local connection into the home router/default gateway. This doesn?t need any additional parameters to be configured as it is a simple test to the local router, however, we recommend leaving the randomized delay in at the start the default of 60 seconds so that not all clients execute this at the same time.

The one input parameter, **MaximumDelayInSeconds** is the Maximum random delay set to avoid network overload. This defaults at 60 seconds and we recommend leaving at this value as this test is only to the local gateway of the employee, it does not impact the corporate network.

Get Network Speed

This Remote Action will determine the speed, in terms of the Round Trip Time, to a given URL and report this back. It also gives Boolean outputs for whether this is greater than the threshold that is requested enabling dashboarding of this property.

Two input parameters define whether this is a public URL or a Business URL. In fact, these are interchangeable, they are just functional guidance, i.e. you can leave two external sites, two sites that are internal to your network, it's entirely flexible, they are just two URLs. The Remote action will test the round trip time to these two URLs and report them.

The configuration required is simply to ensure that the URL?s are configured and once again think closely about what is being tested ? if the test goes down the VPN to the URL then it's not a test of the internet latency direct from the home network, it?s a test of the latency to that URL which (if this is the intended configuration) may well be a web service in a data center. If it goes to a public URL such as google it is more a test of the response time of their device to the internet. A threshold defines the level at which the RTT is considered too slow and marked as bad for that test run.

When public Round Trip time is higher than the average set in the threshold it is a sign of a bad connection. We recommend executing the Remote Action frequently because connection quality can change during the day. Note that you do not have to give both parameters, you can configure one only if wished.

IMPORTANT: From a dashboarding perspective from this pack, this RA also returns the value ?Connection Type? which is used in a lot of the dashboarding, so it is important that this RA is running at least daily to keep the dashboard reflecting the correct data for all RA?s in the pack. Ideally, as this is low bandwidth, it should be run more frequently (hourly). Note that the Connection Type property can be Wired, WiFi, Cellular, or ?Unknown?. This last type may be encountered in certain VPN configurations where Nexthink cannot retrieve the VPN configuration with guaranteed certainty, so shows Unknown in this instance as a reflection that we cannot guarantee what we have found.

There are some parameters to note:

- **MaximumDelayInSeconds**: Maximum random delay set to avoid network overload. Provide the number of seconds lower than 600, Nexthink recommends setting this between 60-300 seconds to balance getting prompt results with overloading the environment with multiple devices querying the destination at once.
- **ExternalURL**: The external URL to check the Web RTT against.
- **WebRTTThreshold**: The time threshold for the external URL Web RTT. Nexthink can recommend a value here, such as 600ms, however, it is going to be very specific to the customer environment. We recommend setting this according to your needs after running it with the default parameter of 600ms and seeing

which values are coming back from your devices. Note that there is a dashboard metric, ?Home Networking - Internet Connectivity - Devices with high RTT to external URL? which also uses this threshold in its calculation so if the value is changed in the RA, please update the metric accordingly. This also applies to the equivalent metric which covers the Business URL.

- ◊ **BusinessURL**: The URL in the corporate environment to be checked the Web RTT against
- ◊ **BusinessWebRTTThreshold**: The time threshold for the business URL Web RTT, please see above for ?WebRTTThreshold? for guidance on this parameter.

Get Download Speed

The Get Download Speed Remote Action downloads a file placed on a cloud service or a file share and will then calculate the speed of the connection based on the time taken to download this file. Please note the file is not fully downloaded to disk, it is simply streamed to the local device and the calculation made.

It will use whichever interface is configured for this destination. Note that with the possibility of UNC and URL-based locations that can be specified, ensure that you understand the configuration needed on the client to make sure you go in the right direction for each download.

VERY IMPORTANT:: This Remote Action downloads a file. There is a randomized delay as per normal that can be set up to 600 seconds however if run across a wide range of devices be absolutely sure that you understand what is happening. It is the intended behavior but particularly for files placed on UNC locations consider that many machines may download this at the same time. It is why we recommend a 50-100Mb file as the optimal size if network capacity allows it.

There are three parameters to understand:

- ◊ MaximumDelayInSeconds: Maximum random delay set to avoid network overload. Provide the number of seconds lower than 600. This parameter should be left high because this Remote Action can

absorb significant network traffic, so having all devices execute at the same time is not desirable. We recommend leaving this at the maximum, 600, which will mean it may be up to 10 minutes before the Remote Action completes.

- ◊ BusinessServiceUNC: Path to a file located in a corporate network's shared location. Eg. \\server\\SharedFolder\\file.txt. IMPORTANT - Do not use a large file or this could flood your network. Provide an empty value to skip this test. Nexthink recommends a value of between 50-100Mb for optimal results of this Remote Action if your corporate network will allow it.
- ◊ BusinessServiceURL: URL to a file located on a cloud location which will then be downloaded to perform the speed test. IMPORTANT - Do not use a large file or this could flood your network. Provide an empty value to skip this test. Nexthink recommends a value of between 50-100Mb for optimal results of this Remote Action if your corporate network will allow it.

The following steps now go into how to configure the files which will be downloaded in more detail. If you are not planning to use this Remote Action these steps can be skipped.

Get Download Speed Remote Action ? Creating the Test File on the Cloud

The Get Download speed Remote Action downloads a file placed on a cloud service. It will use whichever interface is configured for this destination. Note that with the possibility of UNC and URL-based locations that can be specified, ensure that you understand the configuration needed on the client to make sure you go in the right direction for each download.

NOTE: This example uses Azure, however, any cloud storage is possible, for example, AWS. Ensure that the client devices can reach the file destinations, both the UNC and HTTPS (if both are configured) otherwise you will get a failure to connect the message. The Get Download Speed Remote Action has both HTTPS and UNC parameters for both files on the cloud and files on a file share.

Cloud Test File Configuration

To configure this component a file must be placed on a cloud service that can then be downloaded. It should not be too big (we recommend about 50Mb) and it is mandatory that it has open access because the mechanism to download the file needs to be unauthenticated. The following steps outline how to achieve this using Azure, though any cloud provider can be used.

1. log into the Azure Portal (this example uses Azure but any cloud provider can be used).
2. In Any Resource group you wish, create (by clicking on the ?+? sign) a new object of type ?Storage Account?:

   note the importance of the location field for where it will be based and how it will be accessed (https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy).
3. Set the properties of the storage:

4. Continue the wizard to describe the properties of the storage account in terms of networking, data protection, advanced settings, and tags. This is entirely dependent on your choice as an organization, please consult your Azure, AWS, or other cloud service team if in doubt.
5. Finally click on Create in the Review and Create to create the storage.
6. Go to the storage and go to Storage Explorer (Preview) and select Create File Share. Note that you can also create a Blob Storage to do this also (in this case make sure you enable anonymous access in the wizard).

7. Create a file share with a suitable name for your Remote Action test.

8. Refresh the page and now you are able to upload a file into the share:

9. Upload the file you wish to test from bearing in mind that too small may give inaccurate results, too large will potentially congest your network. This can be as you wish, here at Nexthink we recommend 50-100MB for the most optimal results. Due to the way the file is streamed to the client (though not actually downloaded) it must be a .bin extension. This does not have to be a real binary file, it can be something harmless like a text file renamed. If you use other file types you may receive an error in terms of MIME type when the remote action executes.
10. Once uploaded refresh the page, the file is now there in the file share. Now right-click on it and choose Get Shared Access Signature and set the length of access to where you desire:

11. Once created now copy this URI

12. Now paste this into the parameter field in the Remote Action for the BusinessServiceURL:

Get Download Speed - UNC Parameter

A UNC parameter can be specified for the DownloadSpeedUNC. In this instance, the configuration is much simpler but again care must be taken. Firstly, if you configure this property make sure that the device can get to the UNC location, if not, the RA will fail. Once you are sure of this, the UNC parameter, in the simple form of \\server\share\filename is specified. The Remote Action runs in the

context of the current user, so they must have access to the share. With this configured, the RA will execute successfully. Note that for this Remote Action, the Maximum Delay in Seconds should be 600 so that there is a randomized start to the activity so as not to flood the network.

Get Wifi Signal Strength

This will check the signal strength of the WiFi connection and report it back. It will also work on a threshold (configurable) of **AcceptableSignalQuality** which indicates the signal strength that must be reached to be considered acceptable as a percentage. If below this signal strength on each execution it is noted by the Remote Action and if the number of times this occurs in 24 hours passes the **AlertUserAfterBadSignals** value then there is a campaign attached to this that informs the user of how to get a better WiFi signal. This campaign is very basic, and the idea is it can be evolved as wished. If your customer wishes to use it, it is a good idea to upgrade it to a relevant set of campaign statements for your environment. We recommend running this Remote Action regularly so that the Wifi signal is tested regularly throughout the day, ideally hourly.

A number of parameters are available for this Remote Action:

Connection

- **CorporateNetworks**: Comma-separated list of SSIDs which are defined as corporate. It can be empty
- **AcceptableSignalQuality**: Minimum signal quality percentage to consider the current wireless network as good (0 to 100), Nexthink recommends a value above 80 here.
- **AlertUserAfterBadSignals**: Number of times (1 to 200) the signal has to be under the acceptable threshold during the current day to notify the user via a campaign. This will depend on how many times you wish to run the Remote action. Nexthink recommends running this hourly, so on a given day there will be 8 samples taken, so if this value is set to 4, then 50% of signals over the course of a day would have to be poor and it would trigger

the campaign.

- **CampaignId**: Campaign to show with recommendations such as getting closer to the router. Use an empty GUID (00000000-0000-0000-0000-000000000000) to avoid the campaign.

Get Wifi Signal Strength: Co-Channel interference

If a remote worker is in an environment in which there are multiple networks operating on the same channel, congestion occurs in that channel. This congestion results in slow network speeds and reduced productivity. Below is a diagram of a home networking setup that can cause Co-channel interference:

In the context of home networking, if a remote worker has multiple networks sharing the same channel, this decreases the network throughput and reduces the overall quality of their home networking experience. The following measures can be taken to avoid Co-channel interference:

- To fix the issue the competing access points should be moved to a new channel so they don't interfere. There is a Campaign within the pack that can be sent to the employee advising them how to improve their wifi signal strength, which by default advises them to move closer to the access point. This can be enhanced if there is co-channel interference with some advice to reconfigure one of their access points to point to a new channel. NOTE: The steps to do this will depend on the access point type which may vary per employee."

- If the employee is running a 2.4ghz WiFi network, the campaign can be modified to advise them to move to 5ghz (if range allows it, as 5Ghz has less range). Likewise, it can be a good idea to modify the strength of the signal if one of them is weak. Note: If the employee's WiFi routers support mesh networking, this should automatically reconfigure the WiFi networks so this issue should not occur. This would be the best solution but may come at a cost for the employee. Additional solutions can be to move the access points further away from each other and to keep a 20 dB received signal strength indication (RSSI) or more between networks on the same channel.

- **Adjacent-Channel interference**

  If a remote worker is in an environment in which there are multiple access points broadcasting on overlapping channels, data corruption, and transmission issues occur. This will result in poor signal quality and subsequently a lower home networking experience. The following measures can be taken to avoid adjacent-channel interference:

  - Move access points further away from each other.
  - Use the 5GHz band to increase the amount of non-overlapping channels to 24. If only the 2.4 GHz band is available, use the non-overlapping 1, 6, and 11 channels.

The parameters that are relevant to cochannel interference are:

- **NearbyNetworksAcceptableSignalQuality** is the minimum signal strength, as a percentage, that a competing network must be at to consider for analysis as to whether it has an overlapping channel with your current Wifi network. So for example, if you have a Wifi network that has the same channel number as your current one (i.e. will interfere) but you have an acceptable signal quality value of 20% and the competing network is only at 20% then it will not be counted. This is because often in cities there are many low strength networks present.
- **NearbyNetworksMaximumSignalDifference** is the difference in signal strength that must exist for the analysis to complete. For example, if the signal strength of your network is 80% and a competing network is at 20%, but the maximum signal difference is 50% then this will not count because 80-50>20. If the competing network were at 40%, then it would (80-50<40). This factor is used because there must be a significant strength for wireless networks to actually interfere with your signal.

It is recommended that this RA is run regularly, ideally hourly, so that single bad signals do not interfere with the results, i.e. the values are sampled regularly during the day.

Optional - Geolocation RA

This RA is not part of the Home Networking pack but may be used if wished. The purpose is to give more information about where the local connection is originating from. The Geolocation RA has been updated so that it can return more than just the location, it can now return the ISP name which is useful for

customers who want to know which ISP?s are in use.

The RA uses a service from a third party, ipapi.com, which has services ranging from free to paid subscriptions, paid monthly. The use of ipapi.com has been approved by Nexthink Security and Compliance. The free service allows location lookup and up to 10000 executions per month. This has been around for some time at Nexthink as an RA and is still available to use and the Remote Action will still work.

Should you wish to retrieve a greater range of information there are paid subscriptions that can be used. Note that it is customer-centric ? the customer should subscribe themselves to the plan they wish, they will then receive a key that can be used as a parameter in the Remote Action. If a subscription level of ?Standard? or above is chosen then the Remote Action will now return the ISP as part of the returned data, which can be useful for customers who want to look at home networking from this particular angle.

IMPORTANT: An absolutely key point here is that the route to *.ipapi.com should go out of the correct interface in a split tunneling configuration. In the event that the customer uses split tunneling, the traffic must go out of the internet-facing interface and not the VPN interface. If it goes out of the latter you will only get the ISP of the Business as it is really going out of the Business?s gateway. This may well require the addition of this URL to the proxy.pac (or whatever autoconfiguration URL is being used) on the devices that are to run this RA.

- **Get Geolocation** ? Note: Not part of the core Home Networking pack ? is used to give location information on the connection and also optionally ISP details.

    - APIKey: API key to be used for the external geolocation service
    - HTTPS enabled. Valid values are true/false
    - Maximum random delay set to avoid external API overload. Provide the number of seconds lower than 600

Scoring

The pack has a custom Nexthink Score for connectivity (the Connectivity Score). This is a standard Nexthink Score that is targeted at Physical Desktops and Laptops. The score can (and is recommended) be customized as per the normal Nexthink configuration. An outline of the score is described below, it is taking each Remote Action output and summarizing up into an overall score describing both the local and network connectivity.

Change Log

V1.0.2.0

Fixed "Get Wi-Fi Signal Strength" Remote Action data retrieval by obtaining the numeric values in the right format. The pack now has full feature parity between macOS and Windows.

V1.0.1.0

Fixed "Get Network Speed" Remote Action.

V1.0.0.3

Initial publish to the public library.

V1.0.0.2

Updated default values for "Get Network Speed" Remote Action and added warning message for "Get Download Speed" Remote Action.

V1.0.0.1

Fixed category

V1.0.0.0

Initial release

Change Log and Upgrade process

Change log

The Remote Worker Experience pack is currently being regularly updated.

V6.1.3.0

Added "Get Wi-Fi Signal Strength" Remote Action for macOS and updated "Get Wi-Fi Signal Strength" Remote Action adding dynamic parameters capabilities to 'CorporateNetworks' input parameter. The Pack now has full feature parity between macOS and Windows.

V6.1.2.0

Fixed "Get Wi-Fi Signal Strength" Remote Action data retrieval by obtaining the numeric values in the right format

V6.1.0.0

Version 6.1.0.0 enables metrics in the pack to be compatible with macOS systems. These metrics have also been updated to be compatible with the latest version of DEX V2. Additionally, two new remote actions: "Check Certificate Validity" and "Get Encryption Information", for macOS have been incorporated into the pack.

The Check Certificate Validity Remote Action allows administrators to determine if valid certificates are installed on the macOS device and the number of days until they expire. The Get Encryption Information Remote Action determines if the target macOS device's disk is encrypted or not, the encryption method used, and if FileVault is enabled.

V6.0.0.0

Version 6.0.0.0 increases the visibility of Windows 10 from a remote working perspective.

The pack gives a view of the version dispersion across the landscape and for each version it finds, delivers the key metrics needed - whether there are high memory errors, warnings, crashes, and so forth.

In addition, it focuses on changes in the Digital Experience Score on these different versions of Windows 10 if the Device has recently received software updates. It is quite possible an incorrectly behaving update may affect the Digital Experience of the Windows 10 user so by comparing the Digital Experience Scores of machines that are recently updated you will be able to quickly isolate any problems occurring following an update being received.

V5.0.0.0

This update adds a new ?Monitor ? O365 ProPlus? dashboard to the pack which looks at the compliance of Office 365 ProPlus's continuous patching cycle, focusing on remote workers. This dashboard provides valuable insight:

1. Tracks the progress towards patching the Office365 landscape to a desired level of compliance.
2. Breaks down the productivity DEX Score by users on the required patch version compared with those with an outdated version.
3. Gives an overview of the current state of Office 365 ProPlus version dispersion in the landscape.

Outside the core Remote Worker packs note that there is also remote working updates to the separate Device Compliance Pack:

1. Breakdowns by worker type (office/remote) for each dashboard.
2. Critical new software compliance insight, such as top forbidden binaries and breakdowns of non-compliance software at a particular version level (for example a zoom version is known to cause audio lag).

This can be installed at any time independent of the Remote Worker pack itself if wished.

V4.0.0.0

In version 4.0.0.0 of the Remote Worker Experience pack, the following additions are present:

1. In the "Monitor - Compliance" Dashboard key security KPIs are present: Antivirus, Windows Firewall Real-Time Protection, and whether User Access Control is enabled for better coverage of the key aspects of your

remote landscape.
2. As a separate, optional Library Pack, the Windows Defender Management pack has been updated with more dashboards, greater detail, and a breakdown of the Defender status for Office and Remote Workers.
3. As a separate, optional Library Pack, the Level 1 and Level 1 Advanced Checklists have now got several Remote Worker checks in them, such as Wi-Fi Signal Strength, Certificate Check, Password expiration, and more.

Note that the Defender and Checklists are entirely optional items and the Remote Worker Pack can be downloaded by itself if wished.

V3.3.0.0

In version 3.3.0.0 of the Remote Worker Experience pack, the following additions are present:

1. Bitlocker status has been added to the Readiness dashboards (both Assessment and Compliance). Using the Get-BitlockerStatus Remote Action. Note that this can be combined with the equivalent Set remote action to encrypt disks remotely if required.

V3.2.0.0

In version 3.2.0.0 of the Remote Worker Experience pack, the following changes should be noted:

1. The metrics around "Remote Worker Experience - Well-being" will offer to upgrade, this is because of a bug fix around the grouping which has no effect on the UI, therefore if you wish to keep your existing data you can skip this.
2. The dashboards have been renamed and re-ordered in the Portal to make them clearer and more intuitive, they have been given descriptive precursors such as Readiness, Monitor, and Sentiment. One of the side effects of this is that when an upgrade from a previous version takes place, Finder may create empty folders with these new names as it is programmed to keep existing metrics in their current folders. This has no impact on functionality, we would recommend customers to move their metrics from the legacy named folders to the news ones aligning with the portal dashboards and then they can safely remove the old folders.
3. Minor typos in the campaigns.

V3.1.0.0

In version 3.1.0.0 of the Remote Worker Experience pack the following changes should be noted:

1. Wifi Experience is now measured. The dashboard uses both a Remote Action and a Campaign to populate the Wifi data so please ensure if you want to measure this you have targeted and enabled the Remote Action and Campaign accordingly. See below for details on these steps.
2. Minor bugfixes ? minor changes to the text on 2 KPI's.

V3.0.0.0

In version 3.0.0.0 of the Remote Worker Experience pack the following changes should be noted:

1. There is a new category, ?Unwanted Domains? which lists domains or categories of websites that it is preferred people do not visit, not necessarily because they are banned, but perhaps to save bandwidth. This category can be populated with tagging conditions that you wish, such as wildcard site names, domain categories, and so forth.
2. New Dashboards exist for monitoring application metrics and user experience technical data such as response times. There are a number of TopX widgets allowing you to address any high consumption, unstable, or slow responding items.
3. Employee Wellness Campaign. This Engage Campaign targets Remote Workers with a wellness questionnaire to understand how they are feeling when working remotely. It is a non-IT related campaign and will give an indication of employee satisfaction outside purely the IT spectrum.
4. In the existing Satisfaction campaign, there are 2 additional choices to the question "Which of the following issues do you experience when working remotely?": VPN-related issues and Slow or unstable internet connection.

V2.0.0.0

Please note that in version 2.0.0.0 the following changes are important:

1. The Application Category ?Home Office ? Applications' has been removed. This category is superseded by categories for both packages and for executables for the covered applications. Please see below for the configuration of these packages. If you are upgrading from the initial release of this pack, please re-populate the new categories with any additional packages or executables you wish to cover (details further

down).
2. MacOS support is added where possible. Note that not all the dashboards fully support the range of data collected with regards macOS so take note that some dashboards may be partially Mac and Windows and some widgets just Windows.
3. Zoom is added. As with the previous version, only use what you need ? if you wish to remove any of the Zoom, Skype for Business, Teams, or the various Firewall or VPN apps you are more than welcome to do so. Details on this procedure are below.
4. Finally, as with the earlier pack, take particular note that the automatic detection using the IP address uses a feature (last local IP) that is only available since version 6.24 of Nexthink and only when the collector is using TCP as its communication channel. If your environment is below this level, or still uses UDP, then please uses the manual categorization of the User class, to identify your remote employees.

Upgrade process

When upgrading a Nexthink Library Pack from one version to the next, particular care should be taken. Follow this link to read about the upgrade process from a version of a Library Pack to the next one.

Once you have read and understood this process, please return here for specific instructions regarding this pack.

Post V1.x Upgrade

If you have upgraded from V1.x then there are some objects which will remain in place after the upgrade which are no longer needed, these can safely be removed:

Type	Name	Reason
Module	Remote Worker Experience	Replaced by the new module
Module	Remote Worker Services	Replaced by the new module
Category	Home Office ? Applications	Replaced by new categories
Metric	Remote Worker Experience - Readiness Assessment - ALL Ready Users	Obsolete
Metric	Remote Worker Experience - Readiness Assessment - ALL Not Ready Users	Obsolete

Metric	Remote Worker Experience - Sentiment - Positive points	Obsolete
Metric	Remote Worker Experience - Sentiment - Users enjoying work remotely	Obsolete
Metric	Remote Worker Experience - Sentiment - Users not enjoying work remotely	Obsolete

Post V2.x Upgrade

When upgrading from V2.x, there are a large number of metrics that will conflict mainly due to the inclusion of MacOS in the criteria, plus the use of the new categories (mainly Readiness Assessment and Understanding Remote Landscape). You must choose to Replace as the menu option for all content which will align the criteria and configuration to the new pack and use the new categories where relevant. Any customizations made will need to be re-entered.

Remote Worker vs Office Worker Device Category

This category will tag devices as remote based on their IP address. It works on the principle that ranges for workers that are on site ("Office Based Worker") is defined and automatically detected, with any other address considered being remote from the environment and so defining the worker as a "Remotely Connected Worker".

To successfully use this category, please define the ranges that your organization uses when employees are present at the office, i.e. not remote. It is important that the "Last Local IP Address" subnet ranges match the IP configuration for your business.

So, for example, if you use a 10.x.y.z address for your internal addressing when in the Office, ensure this is set in this category. It is pre-populated with 10.x.y.z and 172.16.y.z as these are commonly used for internal addressing when at work. TIP: you can also use "not in subnetwork" to exclude particular ranges that might be within a larger range.

Please note that the automatic detection using the IP address uses a feature (last local IP) that is only available since version 6.24 of Nexthink and only when the collector is using TCP as its communication channel. If your environment is below this level, or still uses UDP, then please uses the manual categorization of the User class, to identify your remote employees.

Finally note that there is no fixed reason that this method has to be used. If you wish to remove the dynamic criteria and simply statically assign a portion of your

devices with this category, this will also work.

Remote Worker Insights

Overview

This solution pack is an addition to the Remote Worker Experience solution, however due to the nature of the pack and the possible side effects if it is misconfigured, it is being delivered as a separate pack, which can easily be merged into the main Remote Worker Experience pack if required.

You cannot download this pack directly from the Nexthink Library you must ask your Nexthink representative to supply it to you.

Pack Contents

The pack is just one dashboard and two metrics supporting them, however it contains an important Remote Action which feed the metrics, **Get Internal Network Speed**. As usual with Nexthink Remote Actions, these should be targeted and run against devices on a scheduled that is wished, however more detail on how it works now follows.

Get Internal Network Speed

Get Internal Network Speed must be executed carefully. This Remote Action takes a Universal Naming Convention (UNC) location for a file share and downloads a file from it for every execution. This is particularly useful for understanding the speed and latency being experienced in terms of getting to the Datacenter of your organization (assuming this is where the file is shared from). High round trip times here are likely to be leading to a poor user experience.

Firstly, the device must be able to reach the share location. In most cases this will be through some kind of VPN connectivity to your organizations network. Once there, the download will take place. Therefore, while this gives a good indication of the latency experience for users, extra care must be taken: all users are reaching the same point and may be going through the same VPN. Ensure that this is not run frequently against many machines at the same time and keep the file that is downloaded to be small (1MB would be ideal). Should too many machines run this at once, or should the file be large, you have a **significant chance of flooding your network**.

Merging the Dashboards

Due to the nature of this pack, we have included it as a separate library pack from a dashboard perspective. However, you will notice that it is included in the **Remote Worker Experience** pack from a Metric perspective. Should you wish to move the dashboard into the Remote Worker Experience pack you can simply use Nexthink's ability to Copy and Paste dashboards between packs to copy the **Monitor - Connection Speed** dashboard into the **Remote Worker Experience** pack.

Category Configuration

The pack uses the Remote Worker vs Office Worker Device and Remote Worker vs Office Worker User categories in the three metrics to give a view of remote connections. One of these categories should be configured as per the documentation links provided.

NOTE: If you have already imported the **Remote Worker Experience** pack then as per normal behavior, these categories will already have been defined by you and no further change is necessary.

Compliance

Device Compliance

Overview

The Device Compliance pack gives an understanding of device compliance from multiple aspects across your device landscape. With dashboards for how well protected your devices are, system, software and network compliance the pack gives a complete picture.

Each aspect of compliance is tracked and scored so that a simple numerical value can be used to understand your compliance status for that area. In addition, there are breakdowns by multiple angles, such as whether your devices are local or remote from the Office, by device type, by location, by model and by OS.

There are some compliance aspects that function immediately that the pack is installed and some that require a small amount of configuration, which now follows.

Configuration

The pack uses a number of categories, which should be configured according to the needs of your Organization.

Compliance (Binary Category)

NOTE: This is the binary category as there are multiple categories called Compliance. In this category there are three tags to represent the corporate browser, binaries that should not be present at all (no matter what version) and binaries that are considered non compliant if they are beneath a certain version. Please populate according to your corporate needs.

Compliance (Domain Category)

This contains the list of white listed (allowed) or forbidden (blacklisted) domains for your corporation if you wish to list them. The pack has dashboard's showing the compliance regarding devices visiting these domains.

Corporate AV

This category is to be populated with the corporate Anti-virus that is used at your Organization under the "yes" tag. The "no" tag should be left to all other matches so that it is either finding the Anti-virus or not.

Corporate AS

This category is to be populated with the corporate Antispyware that is used at your Organization under the "yes" tag. The "no" tag should be left to all other matches so that it is either finding the antispyware or not.

Corporate FW

This category is to be populated with the corporate Firewall that is used at your Organization under the "yes" tag. The "no" tag should be left to all other matches so that it is either finding the firewall software or not.

Local admin white list

This category defines devices where it is approved to have admin privileges. Manually tag any devices to which this applies according to your corporate policy.

Proxy White list

This category defines devices where it is approved to reach external destinations. Manually tag any devices to which this applies according to your corporate policy. If you have a corporate policy allowing all devices of a particular type (for example, workstations and laptops) to access external destinations (e.g. the internet) then use a dynamic rule to include these types of devices.

OS Compliance

This category is to be populated with the corporate Operating System(s) used at your Organization. The dashboard will show any non compliant devices from this perspective.

OS Name

This category groups operating systems together, as you introduce new Operating Systems into your Organization please add new tags for it.

Type (Application Category)

This category is for applications by type, please group your applications according to the relevant type.

Model

This category groups different model's of device together. Please ensure the groupings match your Organization hardware device types.

Remote Worker vs Office Worker Device

This category will tag devices as remote based on their IP address. It works on the principle that ranges for workers that are on site ("Office Based Worker") is defined and automatically detected, with any other address considered being remote from the environment and so defining the worker as a "Remotely Connected Worker".

To successfully use this category, please define the ranges that your organization uses when employees are present at the office, i.e. not remote. It is important that the "Last Local IP Address" subnet ranges match the IP configuration for your business.

So, for example, if you use a 10.x.y.z address for your internal addressing when in the Office, ensure this is set in this category. It is pre-populated with 10.x.y.z and 172.16.y.z as these are commonly used for internal addressing when at work. TIP: you can also use "not in subnetwork" to exclude particular ranges that might be within a larger range.

Please note that the automatic detection using the IP address uses a feature (last local IP) that is only available since version 6.24 of Nexthink and only when the collector is using TCP as its communication channel. If your environment is below this level, or still uses UDP, then please uses the manual categorization of the User class, to identify your remote employees.

Finally note that there is no fixed reason that this method has to be used. If you wish to remove the dynamic criteria and simply statically assign a portion of your devices with this category, this will also work.

GSuite

GSuite: Health

Pre-Requisites

This pack has no mandatory pre-requisites and can be run directly without configuration. However optional configuration may be necessary as described below.

Defining Additional Domains

Configure Category '**GSuite Web Apps'** if you have your corporate domain or domains designated as GSuite domains. So for example if you have mail.domain.com set up as an alias for GMail (mail.google.com) then you can optionally add these domains to the Category so that both domains will appear in any results concerning metrics relying on this category.

GSuite: Services

Overview

This pack is made up of a number of Nexthink Service definitions covering all the main GSuite Workloads. There is no mandatory configuration, however optional configuration can be made:

Configure Additional Domains

If your Organization has configured your corporate Domain(s) to be managed by GSuite, then you can add these domains to the Category '**GSuite web apps'** to indicate any additional Domains as required for the various GSuite Services.

Configure Alerting

Should alerting be wanted when a threshold is breached for a particular service this can be set up for each service within the pack. There are a

number of options around how services can be configured within Nexthink so please follow these instructions for each Service that you wish to configure this for.

GSuite: Sentiment

Pre-Requisites

This pack uses Nexthink Engage campaigns. As such some configuration is required to ensure the campaigns are targeted suitably. Each Campaign is discussed below.

GSuite - New Service Arriving

Configure Campaign **GSuite - New Service Arriving** if you have a new or Service (or just if you want to inform users of change to one of the existing GSuite Services). There is not specific set of users targeted with this Campaign, it is your choice.

First you must edit the Campaign and insert in the description exactly what you would like to say to users, including any hyperlinks you might need. Once this is done select '**Publish'** from the menu. Because it is a manually targeted Campaign, next go to the Investigations area in the Finder and make a user based Investigation targeting whichever users you wish to receive the Campaign. As an example we have included an Investigation '**GSuite - Users using Google Chrome'** which can be used if wished. Once you have the results, i.e. your target user set, right click and from the context menu and select the campaign to deliver it. *Make sure you get the list of users correct so as to not deliver to users not expecting the Campaign*.

Note that once published you can edit the description and content of the Campaign to amend it for new services being delivered.

GSuite - Service Outage / Service Resolved

Configure this Campaign when there is a planned or unplanned Service Outage. The process is exactly as described above for the '**New Service Arriving'** Campaign, however with two Campaigns, both the announcement and the resolution campaigns, ensure that you send the right campaign to the right users for when the service outage occurs and

when it is resolved.

GSuite - Production Feedback

This campaign is a general feedback Campaign for users of the GSuite service. It indicates overall satisfaction with the Service. As above, the Campaign should be manually targeted to a group of Employees if to be delivered one time only. This campaign could also be run regularly to Employees to continually understand the Sentiment of users and any happiness or unhappiness with the Service.

If you wish to change the Campaign to be a regularly running campaign it will need to be altered to be targeted with a suitable investigation for your target users. For more information on this process please see the relevent documentation

GSuite - Audio or Video Call Quality Satisfaction

Unlike the previous Campaigns, this Campaign is intended for continuous feedback on G Suite call quality and Video quality. Examine the Campaign details in terms of the title and description amending as wished. When ready, publish the Campaign. It is targeted at the Investigation '**GSuite users with audio or video calls in the last hour'** so when published this Investigation will be evaluated and continue to be so every 10 minutes following. The Campaign is configured so that no recipient will get the Campaign more than once every six months.

This configuration is flexible. If you wish to change it to be manually targeted you are free to do so.

GSuite: Advanced health

GSuite: Advanced Health

Pre-Requisites

This pack does not have mandatory pre-requisites but does use Remote Actions that must be configured. Upon import the 'Test Chrome Plugin Compliance', 'Get Browser Tabs' and 'Get Chrome Plugins' will be created.

Chrome Compliance

This pack concentrates on Google Chrome

It starts with how much of your landscape does and does not have Chrome installed for a high level view on your Chrome Deployment.
Following this, there is information on the success of the "Test Chrome Plugins Compliance" Remote Action, which should be run on a regular basis. This Remote Action will check whether given Plugin's are present and at what version. Should this check be failing, it should be investigated on these devices. Make sure that this Remote Action is configured to run at a suitable frequency, ideally daily and that in the input parameters you have configured which plugins are to be tested and whether to go to the version level or simply test for presence.
Next the dashboard will show how many devices that successfully ran the check, returned compliant or not compliant, i.e. a successful technical execution, now looking at the results. Should anything be non-compliant there is need to look at the Remote Action output in the Finder to find out why they were not compliant.
After this, there is Individual Plugin Compliance Failure, showing devices that have successfully run the Remote Action, returned not compliant and now showing which plugin had returned non compliant. Any devices should be investigated.
In all the above scenarios, the dashboard and metrics are using basic checks on the base plugins (gmail, docs, sheets) however the RA can be very granular, it can look for any plugin at any version and whether it is enabled or disabled. Should you wish to customize this dashboard or the metrics behind to suit your organization then the criteria's can be customized as far as is needed.
Should more than one Compliance profile exist, then it is possible to duplicate the remote action and give a second set of criteria in the duplicated Remote Action.

Defining Additional Metrics

This Pack is very dependent on individual environments. The metrics that are part of the dashboard are meant only as a starting point for configuration, looking at the most basic options.
Should your organization have a different set of plugin's or version levels then feel free to create new metrics as described above with alternative criteria from the output of the Remote Action.

Support

Support: Level 1

Level 1: Checklist

The Level 1 Checklist contains a number of key checks that can be used by Level 1 ServiceDesk staff to quickly gain a single pain of glass view of a device and understand at a glance the key digital experience key indicators. Each L1 checklist item is scored according to a value and as such when the score is too low it will be shown as red, a green visual indicating a score that is an acceptable level.

Level 1: Checklist Advanced

The L1 Checklist Advanced takes the L1 Checklist and extends it to include various checks that are performed by Remote Actions. For added security, the library pack by default imports remote actions with manual execution disabled. To enable manual executions edit each remote action, and check "Allow manual triggering of the remote action on these devices". Optionally, select a category & keyword to limit the execution on a set of devices only.

Shadow IT

Shadow IT

Overview

Shadow IT is a term often used to describe IT systems and IT solutions built and used inside organizations without explicit organizational approval. Find out more about Shadow IT on the Nexthink blog and Wikipedia.

It is in the interest of any organization from a management perspective to know which Shadow IT tools, if any, are being used by users. This library pack contains metrics with conditions that are configured to detect specific applications that are being used unofficially by active users within your IT environment. You'll also find metrics that aim to return a list of applications that are generating the most web traffic. This will help you in further understanding which applications are most in use.

This information will also help you in understanding the behavior of your users not just by looking at which applications are most in use, but how they are used. For example, included in this pack are metrics that allow you to determine if proxies and even tools like tor are being used by users in your IT environment. If, for example, you're interested in finding out how much users are using tools and services that have been recommended for use under your organization's policies, you can do that with this pack.

Included in the pack by default are metrics that allow you to retrieve a list of users that use a specific application for a specific purpose. These metrics have been separated into groups by use case. For example:

Data storage
: These metrics when executed, return a list of users using storage applications such as OneDrive, Dropbox, Google Drive, Copy, and Box.

Conferencing and VoIP
: These metrics when executed, return a list of users using VoIP applications such as Lync, Skype, GoToMeeting, Webex, and Google Talk.

Productivity
: These metrics when executed, return a list of users using productivity applications such as Office 365, Google Docs, Evernote, Basecamp, iCloud.

Business

These metrics when executed, return a list of users using business applications such as Salesforce, Concur, Netsuite, Workday, Marketo

Pre-Requisites

This pack requires Nexthink Version 6.20 or above.

Change log

V1.0.0.2

Investigations have been removed from the pack because there were conditions that referenced Nexthink Enhance which is no longer supported.

V1.0.0.1

References to Nexthink Enhance components have been removed from some metrics. As a result, some metrics have been removed or altered. Naturally, some dashboards have also been removed or altered to reflect the changes to the metrics.

V1.0.0.0

Initial release.

Configuration

No mandatory configuration is required.

The pack searches for a list of Shadow IT applications. Should you wish to search for different or additional applications within your organization, then the existing metrics within each folder of the Library Pack are searching for particular binaries or applications. Should you wish to search for a new application then the simplest mechanism is simply to **Copy** and then **Paste** the respective metrics and change the binary or application name to the new one you are searching. Of course, should you wish to see this in the Portal then a Widget must be created in addition.

Malware Protection

Malware Protection

Overview

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising (source: Wikipedia)

The purpose of this pack is to help you improve the security in your IT environment by ensuring that your endpoint security tools are installed and working as desired. You'll be able to see which devices do not have Antivirus, Antispyware, and firewalls installed and running. The pack will also help you identify known malware that may have gotten past your defensive systems and is still unknown to your Endpoint protection tools.

Included are metrics configured to identify binaries with suspicious behavior. These metrics will return a list of binaries including their version, MD5 hash, and location on the target system. As shown in the image below, your security teams can use the Finder to drill-down and investigate the behavior of these binaries further.

Pre-Requisites

This pack requires Nexthink Version 6.20 or above.

Change log

V1.1.0.1

References to Nexthink Enhance have been removed from some metrics. As a result, some dashboards have been altered or removed to reflect the changes to some metrics.

V1.1.0.0

Removed digest configuration

V1.0.0.0

Initial release.

Configuration

Before deploying this pack, we recommend going through the metrics in the "Suspicious binaries" folder and refining them so that they are in line with your organization's threat profile. Specifically, the metric "Binaries with suspicious web activity" has been configured to look for only one binary with suspicious web activity. If you wish to look for more specific binaries, we recommend that you create another condition definition within this metric.

Office 365 Health

Office 365 Health: Overview

Office 365 Health: Overview

Pre-Requisites

There are no prerequisites

Defining Tenant Names

It is necessary to amend two categories, SharePoint and OneDrive, so that the URL's correctly point to the relevent URL's for your Organization.

1. In Category folder **Office 365 Health - web apps** configure Category **Sharepoint** and **OneDrive** to give the name of your Office 365 Tenant(s).
2. The "COMPANY_NAME" should be replaced with your tenant name (normally the same or related to your company) so for example **Nexthink.sharepoint.com** or **Nexthink-my.sharepoint.com**.
3. Additional autotagging conditions can be added if you have multiple tenants.

Office 365 Health: Services

Pre-Requisites

There are no prerequisites

Mandatory Configuration

There is no mandatory configuration to be performed in this Module. If any of the Services are not desired to be monitored they can be removed in the normal way by editing the dashboard and removing the widget.

By default all services will be monitored.

Optional Configuration

Should alerting be wanted when a threshold is breached for a particular service this can be set up for each service within the pack. There are a number of options around how services can be configured within Nexthink so please follow the instructions found here for each Service that you wish to configure this for.

Office 365 OneDrive

OneDrive Summary

Overview

OneDrive is Microsoft's Cloud-based file storage solution. Offering large amounts of storage securely, it is popular and growing amongst businesses of all sizes.

Nexthink's OneDrive Solution Packs cover all aspects of a OneDrive deployment, from Migration to Production and on into the Sustain.

The four packs cover different areas of the Product:

1. Operations - This covers the day to day Production run of OneDrive on the client devices. It requires the core Nexthink Analytics module.

2. Advanced Health - This enhances the Operations solution with additional insights into OneDrive gained from deeper analysis using the Act module. It also allows for various proactive actions to be taken through the Remote Actions functionality.

3. Migration - Many organizations are thinking about, or commencing, a migration to OneDrive. This module will take them through this migration walking from the initial readiness through to the Production completion.

4. Sentiment - This Module uses the Engage functionality to add Sentiment analysis to the solution so that the Technical Metrics can be correlated to genuine user feeling. It also enables Out-of-the-Box Service messages for topics such as OneDrive service degradations.

5. Advanced Operations - This Module, like the Operations pack, helps administrators gain deeper insights into OneDrive deployments.

OneDrive Operations

Overview

The Operations pack covers the day-to-day running of OneDrive across Production. The pack has feature parity between Windows and macOS.

Overall Installation and Configuration

The installation of the pack depends on the existing configuration. If you have already installed and are using the existing legacy Nexthink OneDrive pack then the recommended approach is to remove this pack and then install the new 'OneDrive - Operations' Pack. The new Pack will then install silently without conflict.

Should you wish to keep the existing OneDrive Pack then there are some metrics that are common to the two Packs. Therefore you will be prompted on install of the new 'OneDrive - Operations' Pack whether to merge some metrics which are common to the pack. To work successfully with the new Pack please choose "Replace" rather than "Skip" to ensure the best functionality of the new Pack.

There is no mandatory configuration for the pack once installed, it will work as soon as deployed, however there are some optional steps that can be taken if wished.

Firstly, there is a Category "OneDrive Process". This contains both the Windows and Mac versions of the OneDrive process. If there are no Mac (or no Windows) in your environment, then the appropriate classification within the category can be removed.

There is also the categories "Shadow Storage" for which has DropBox and Google Drive File Stream entries for the processes and also the Domain destinations. These can be removed if wished or similarly if you have other non compliant cloud storage provides you would like to add, they can be included by adding another classification within the categories.

Mandatory configuration

- No mandatory configuration is required.
- Optional Configuration as described above may be performed.

OneDrive Advanced Health

This article or section is in the process of an expansion or major restructuring.

OneDrive Migration

Overview

OneDrive is Microsoft's Cloud-based file storage solution. Offering large amounts of storage securely, it is popular and growing amongst businesses of all sizes. Nexthink's OneDrive Solution Packs cover all aspects of a OneDrive deployment, from Migration to Production and on into the Sustain. The Migration pack concerns the transformation of a traditional home folder corporate setup to one that uses OneDrive for Home Folder Storage.

This Library Pack does not perform the migration execution, as there are multiple ways in which an organization will move files into OneDrive, it's aim is to enable smooth management of this process. However, the actual technical file transfer into OneDrive may take place. The idea behind the pack is that users will be split into Waves. These waves will then be migrated to OneDrive sequentially.

Configuration

There are several important key concepts in this Library Pack to be understood and configured.

Legacy Home Folder location

The pack uses the idea that the Personal folders to be moved to OneDrive must exist somewhere on the corporate landscape. This can be anywhere from the local device hard drive, to a server-based UNC Share. As part of the Pre-Migration confirmation that an Employee is ready to be migrated, the Library Pack will need to be configured with the location of the share that is used for an Employee to reach their personal files. This can also be expressed as environment variables, for example **"\\Server1\Home\%Username%"** or even **"%HomeDrive%%HomePath%?** which enables the pack to work for multiple users with a single configuration.

Pre-Migration Pre-Requisites

The Library Pack will perform a number of checks on both the technical data of the user's home directory, finding any files which cannot be migrated to OneDrive

as well as Sentiment based checks using Campaigns within the pack, which will highlight users who are requesting more help.

Home Directory Servers

In the event that the company uses traditional file servers to host the existing Home Folders for users, then these should be populated as part of the category Home Folder Servers and the pack will then highlight the file access traffic going to and from these servers from the user's devices. This is important in the planning of your OneDrive migration. You must make sure that you understand how much traffic is being used for the existing home drive solution so that you can then plan for this traffic to become internet facing traffic when moving to OneDrive.

OneDrive Deployment Wave

The category 'OneDrive Deployment Wave' should be used to move individuals into different batches for migration. Ideally, several batches can exist moving in a train-like fashion, with batches executing as time allows during the migration. The pack comes with a dashboard for one wave, but more can be created as required along with the prerequisite metrics for the new wave(s).

The difference between not being migrated and being migrated is handled via Categories in this Library Pack. Initially, all Employees should be given the category "Unassigned to Wave" meaning they still need to be assigned. Employees should be assigned to either being Excluded or one of the Migration waves as part of the setup. During migrations, once a user has been either moved to OneDrive or failed to move, their category should be set to either "Migrated" or "Failed" depending on the outcome. This is then reflected in the dashboards of the pack.

Remote Action Configuration

There are two remote actions that are included in this Library Pack. Both remote actions are used by several metrics to collect information relevant to the migration process. Information such as file sizes, number of directories, and sub-directories on a local device hard drive or a server-based UNC. One of the remote actions also checks for invalid file paths and invalid file name syntax. For these remote actions to function, they need to be manually provided a path to the local or UNC drive. This is done by going into the finder, finding the remote actions, and editing the **InputPath** parameters as desired. Listed below are remote actions that **must** be downloaded and installed in your finder for this Library Pack to work correctly:

Get User Folder Size

The 'Get User Folder Size' remote action is included in the Windows Information Library Pack.

Test OneDrive Files Path and Syntax

The 'Test OneDrive Files Path and Syntax' remote action is included in the OneDrive Library Pack

Metrics configuration

The metrics included in this Library Pack were built with the assumption that they will be customized to fit the digital environment in which they will operate. Generally, a fair amount of them makes use of the two aforementioned remote actions, especially the Sentiment metrics. Most of them have extensive interaction with the OneDrive Migration Sentiment, OneDrive Deployment Wave, and Home Folder Sizes categories included by default in this Library Pack.

Engage Campaigns

There are three Campaigns of importance: Training, Pre-Migration, and Post-Migration in the pack. These campaigns are configured to manually target users by default but can be changed to make use of the utility of investigations or remote actions.

Training

This Campaign can be targeted at any users who require training either before or after migration, ideally this should be all Employees. The Campaign should be customized to your Organizations needs and requirements and then delivered. As part of this Campaign, the Employee is also asked whether they require more training and if they respond positively this is visible in the Migration dashboards.

Pre-Migration

this Campaign looks at the overall satisfaction with the existing Home Folder solution, whatever it may be. It is important to take this Sentiment before migration to OneDrive so that post-migration, the same Campaign can be run, and it can be determined whether the Employee views OneDrive as an improvement. If they don't then this should be discussed and analyzed within the company, as a migration to a new service like OneDrive should be an enhancement not a detriment to the user. Users who have been migrated should be put into the category of 'OneDrive Migration Sentiment' by attaching the 'Post-Migration Sentiment' tag to them.

Post-Migration

Similar to the Pre-Migration Campaign, this Campaign's purpose is to determine how satisfied the Employee is with their new OneDrive solution. It should be taken following successful migration. This would then allow for administrators to know who views the new solution as an enhancement and who views it as a detriment. Users who have been migrated should be put into the category of 'OneDrive Migration Sentiment' by attaching the 'Post-Migration Sentiment' tag to them.

OneDrive Sentiment

This article or section is in the process of an expansion or major restructuring.

OneDrive Management

Overview

The OneDrive Management Pack enables you to get better insights into your OneDrive deployments. It consists of Remote Actions that return the status of various aspects of your deployment such as the Download and Upload speeds of OneDrive clients on remote devices, the number of OneDrive clients failing to upload files, The size of OneDrive folders, and the Update ring of a device with a OneDrive client installed.

You can remotely configure the Update Ring of a device with a OneDrive client installed by using the "Set OneDrive Configuration" Remote Action that comes with this pack. Additionally, you can Repair or Reinstall a faulty OneDrive client using the "Repair OneDrive" Remote Action that also comes with the pack.

Pre-Requisites

There are no prerequisites to using this pack. Please consult the configuration section below before running the Remote Actions contained in the pack.

Configuration

This pack contains only Remote Actions. The ones listed below will need to be manually configured as they require a value to be passed to their parameter(s). To determine which values must be passed to the script, please navigate to the Remote Action section of your Nexthink Finder and open it. In the section titled "Windows", you will see a description of the script written in green text. in the

"Inputs" section of the text, you'll find a description of the expected values for the Remote Action.

1. Get OneDrive Information
2. Get OneDrive Status
3. Test OneDrive Files Path and Syntax

Change log

V1.0.0.0

Initial release.

Office 365 Teams

Teams Overall Configuration

Create Service

It is strongly advisable to create a Nexthink Service for the Teams Service which provides a lot of insight out of the box of any given process. Note that this only needs to be done once, whereas there are many Teams Solution Packs, so please follow these instructions only once, not once for each Pack. To configure this, go to the ?Services? and configure a new service as you would for any other Nexthink Service definition:

Note the type is HTTP and TLS web requests. This will then, as per normal, create the Dashboard for this automatically within the portal which you can then use.

Follow the evolution of the service in Portal.

Configure categories

- When deploying Teams there are many scenarios where it will be rolled out to an Early Adopter group before being rolled out to the main Production users. In this scenario there is a Nexthink Category which allows you to flag these users as Early Adopters and there is a dashboard relating to this which enables you to look at the Early Adopter statistics compared to the Production users.
- This pack has two important Categories. The first is Teams User Deployment Ring:

- This category defines all users with the Keyword Production unless they are manually categorized as having a different deployment ring, which can be Early Adopter or other Pilot rings.
- The metrics and dashboards as delivered use only the Production or Early Adopter Keywords. If other deployment Rings are needed the metrics can be duplicated and amended accordingly.
- If you are wanting to pilot Teams to a set of users then please set the Keyword on them via the Finder to be ?Early Adopter?:

Tip: If Teams is to be deployed in stages across the Production landscape it is also possible to move the order of the auto tagging so that users are defined as ?uncategorized? and not Early Adopter or Production, meaning they will be excluded from any dashboards until they are then classified as such. This allows for a model where Teams is being slowly deployed across the organization and users can be classified as Teams Production users as the Production deployment takes place.

Once the configuration is in place, then the Dashboards for Overview and Performance will populate with the metrics for the Users that are classified as

Early Adopters.

The second Category that should be noted is "MS Teams". This contains the executable files for Teams on Windows and Mac along with the Teams Updater executables. This should not need configuring, however if you wish to bring in additional executables that are part of Teams to be monitored by Nexthink, this is possible here simply by amending the category.

- Note: If you change a category (new keywords, change of condition, etc.) and import a new Pack referring to it, the ?Finder conflict? dialog will prompt. Select either Merge or Skip in order to keep the changes that you have made.

Teams - Migration

Summary

The Teams ? Migration pack looks at the performance of devices running Teams to allow you to pinpoint any potential issues.

It also has Dashboards allowing comparisons between the Pilot users and an existing Skype for Business deployment.

The four dashboards are split, with two focusing on the Pilot users and two focusing on a Skype for Business migration scenario.

Version History

V1.1.0.0

This upgrade introduces Focus Time which is the Nexthink metric that measures the time that a user has the targeted application window open and active. This gives a good indication that the application is being used and for how long.

Please note that Focus Time is not yet compatible with Focus Time but will be included in the next release

Upgrading from an earlier version

For metrics that refer to the Teams executable, there are new categories that allow the pack to be configured to look for supporting or additional files as opposed to the previously hard-coded entry for teams.exe.

In addition the dashboards have been upgraded to include more helpful and relevant metrics for Teams landscape management.

However, with this level of upgrade, there is a small cost: if upgrading from an earlier version many of the metrics will offer an option of replacing or skipping as part of the pack upgrade. As with standard Nexthink behavior this does mean that if replace is chosen then the metric history will be lost as will any customizations against the metric.

Therefore it is our advice not to upgrade this pack, but to remove the earlier version and install this as a fresh, clean build.

If this is not an option for you as an Organization then "Skip" may be chosen during the import however post customization of the metrics may be wished to bring them in line with the new dashboards.

Whichever option is chosen, post installation, if you wish to rely on the new dashboards only and no longer need the older dashboards, then the following metrics are no longer used:

- Teams - Devices with failed web requests by version - Early Adopters

Because, by design, Nexthink does not delete metrics during an upgrade, these should be removed post upgrade as they are not present in any of the new dashboards.

Overall configuration

Follow the overall configuration for all Teams library packs.

Mandatory configuration

- No mandatory configuration is required.

Teams - Health

Summary

The 'Teams - Health' pack looks at the Production Landscape using Nexthink Analytics. It does not use the Act or Engage modules and it will provide the performance, landscape deployment and adoption information key to understanding your deployment.

Changelog and Upgrade Process

Pre-Requisites

This pack uses metrics from the Digital Experience Score V2.x (i.e. V2.0 and above). This is used on the first dashboard only. Should you wish to view these metrics in the pack, please ensure you import DEX V2.0 or above before importing the MS Teams pack.

Version History

V2.0.0.0

This upgrade brings better categorization so that both macOS and Windows is supported, plus the Teams Updater application is included.

The metrics bring better layout, stronger metrics and the inclusion of the Digital Experience Score for Teams.

V2.1.0.0

This upgrade introduces Focus Time which is the Nexthink metric that measures the time that a user has the targeted application window open and active. This gives a good indication that the application is being used and for how long. Please note that Focus Time is not yet compatible with macOS but will be included in the next release

Upgrading from an Earlier Version

Starting with version 2.X and above, the Teams pack undergoes significant changes. For example, there is macOS support, there are categories underpinning the metrics for the Teams executables enabling freedom to configure the pack to look for supporting or otherwise additional files within the

category instead of looking for the previously hard coded teams.exe as the only option.

In addition the dashboards have been upgraded to include more helpful and relevant metrics for Teams landscape management.

However, with this level of upgrade, there is a small cost: if upgrading from an earlier version many of the metrics will offer an option of replacing or skipping as part of the pack upgrade. As with standard Nexthink behavior this does mean that if replace is chosen then the metric history will be lost as will any customizations against the metric.

Therefore it is our advice not ot upgrade this pack, but to remove the earlier version and install this as a fresh, clean build.

If this is not an option for you as an Organization then "Skip" may be chosen during the import however post customization of the metrics may be wished to bring them in line with the new dashboards.

Whichever option is chosen, post installation, if you wish to rely on the new dashboards only and no longer need the older dashboards, then the following metrics are no longer used:

- Teams - Devices with failed web requests by version - Production
- Teams - Top 20 devices with high CPU usage ratio - Production
- Teams - Top 20 devices with high memory usage - Production
- Teams - Top 20 devices with high network response time - Production
- Teams - Inbound network traffic - Production
- Teams - Outbound network traffic - Production
- Teams - Top 20 devices with high network traffic - Production

Because, by design, Nexthink does not delete metrics during an upgrade, these should be removed post upgrade as they are not present in any of the new dashboards.

Overall configuration

Follow the overall configuration for all Teams library packs.

Mandatory configuration

- No mandatory configuration is required.

Teams - Advanced health

Overall configuration

Follow the overall configuration for all Teams library packs.

Remote Actions

- The Advanced Health solution pack delivers some additional metrics which provide further detail on the landscape. These are provided by Remote Action?s which can be configured to run on an as-needed basis or regularly.
- There are three Remote Actions which can be used:

Remote Action: Get Teams Info

- This Remote Action is found within the Nexthink Library > On Demand area:

- The data returned by the remote actions are:
    - Devices with Connection Issues ? these are devices that have reported a problem connecting to the Teams service within the last 24 hours.
    - Devices with Authentication Issues ? These are devices that have reported a problem with Authentication of the user within the last 24 hours.

- Users Making Calls ? This is a count of the number of calls made by a user over the last 24-hour period.
- Deployment Ring ? This is the Microsoft Deployment Ring if there are users that are members of the Technology Adopter Programme for Microsoft Teams. Note that this is separate and different from the Nexthink "Teams User Deployment Ring" which is entirely configurable by the Nexthink Administrator as they wish.

Remote Action: Reinstall Teams Client

- This Remote Action can be used to initiate an install or reinstall action of the latest version of the Teams Client on the given device.

- The Remote Action will work in the context of the current interactive user, if no user is logged on it will exit.

- If the user is not using Teams then it will upgrade Teams in the background (although note that as part of this Teams executes once installed, which is unavoidable).

- If the user is logged in then a campaign is launched allowing the user the choice of installing Teams, skipping or deferring:

- Once the reinstallation has completed the Campaign closes with a final message confirming it has run and then exits.

Remote Action: Invoke Network Assessment Tool

- This Remote Action executes the Skype for Business Network Assessment Tool. Despite its title, this tool can be used universally to test connection quality for Teams or Skype for Business and is based upon the execution on the client of the free tool directly from Microsoft. When using the tool note that it uses the Teams port ranges to make its check (3478, 3479, 3480, 3481) and as per the Microsoft Port Requirements Page for O365 these must be open as per normal Teams configuration for the tool to work.

- The Remote Action currently relies on the tool being installed on the client, in the default location, therefore before executing the tool it should be deployed via software distribution or manually to as many machines as are wished.

- Once present, the Remote Action should be set to be able to be run on demand and can then be executed against the machine(s).

- The tests will take approximately 30 seconds and the output will be a set of values that determine the quality of the connection.

Along with the actual returned values, the solution also output?s whether these values pass or fail Microsoft?s benchmarks for a suitable quality connection for Teams

- This RA can be run as a one-off test to check quality but also on a regular basis to confirm line quality on a daily or weekly basis.

The Advanced Health data can all be seen on the Advanced Health Dashboards that are part of the Pack:

Teams - Adoption

Summary

- This pack helps measure your employee satisfaction, adoption and collaboration on Microsoft Teams. Track what your employees like and dislike and see how much time is being spent using the tools with Focus Time, and if in the end they preferred the old way compared to the new.
- Four dashboards focus on the Early Adopters and four dashboards target Production.

Version History

V1.1.0.0

This upgrade introduces Focus Time which is the Nexthink metric that measures the time that a user has the targeted application window open and active. This gives a good indication that the application is being used and for how long. Please note that Focus Time is not yet compatible with macOS but will be included in the next release

Upgrading from an earlier version

For metrics that refer to the Teams executable, there are new categories that allow the pack to be configured to look for supporting or additional files as opposed to the previously hard-coded entry for teams.exe.

In addition the dashboards have been upgraded to include more helpful and relevant metrics for Teams landscape management.

However, with this level of upgrade, there is a small cost: if upgrading from an earlier version many of the metrics will offer an option of replacing or skipping as part of the pack upgrade. As with standard Nexthink behavior this does mean that if replace is chosen then the metric history will be lost as will any customizations against the metric.

Therefore it is our advice not to upgrade this pack, but to remove the earlier version and install this as a fresh, clean build.

If this is not an option for you as an Organization then "Skip" may be chosen during the import however post customization of the metrics may be wished to bring them in line with the new dashboards.

Whichever option is chosen, post installation, if you wish to rely on the new dashboards only and no longer need the older dashboards, then the following metrics are no longer used:

- Teams - pre-deployment adoption times - Early Adopters
- Teams - pre-deployment adoption times distribution - Early Adopters
- Teams - pre-deployment adoption hours - Early Adopters
- Teams - pre-deployment adoption hours distribution - Early Adopters
- Teams - post-deployment adoption times - Early Adopters
- Teams - post-deployment adoption times distribution - Early Adopters
- Teams - post-deployment adoption hours - Early Adopters

- Teams - post-deployment adoption hours distribution - Early Adopters
- Teams - pre-deployment adoption times - Production
- Teams - pre-deployment adoption times distribution - Production
- Teams - pre-deployment adoption hours - Production
- Teams - pre-deployment adoption hours distribution - Production
- Teams - post-deployment adoption times - Production
- Teams - post-deployment adoption times distribution - Production
- Teams - post-deployment adoption hours - Production
- Teams - post-deployment adoption hours distribution - Production

Because, by design, Nexthink does not delete metrics during an upgrade, these should be removed post upgrade as they are not present in any of the new dashboards.

Overall configuration

Follow the overall configuration for all Teams library packs.

Categories

- The same campaigns are meant to be sent to "Early Adopters" and "Production" users, but at different times. Therefore, it is recommended to categorize the target audience for each campaign with an additional category "Teams User campaign recipients".

Campaigns

- All Campaigns must be configured with the Sender Name, Title and Picture.
- All Campaigns can optionally be translated, and the display texts can be edited but it is not recommended to change the structure of the campaigns, the type of questions, the names of the answers, etc.

- The company?s logo can be uploaded in Portal to customize the look and feel of the notification.

Step by step guide

Assess who would like to become Early adopter

The first campaign "Teams - early adopters" can be sent to all employees to assess who would be interested in becoming part of the "Early Adopter" program.

1. Create investigation to target recipients. In this case it?s a straight-forward "select all users" investigation.
    1. Create and save an investigation to select all users.

2. Publish campaign
    1. Drag & drop the newly created "All users" investigation into the recipients' section of the campaign

    2. Optionally preview the campaign

3. Publish the campaign

3. Wait for few days/week and view results in the dashboard "Early adopters: Overview".
    1. Go to Portal > Module "MS Teams" > Dashboard "Early Adopters: Satisfaction"

    2. Mouse over the KPI in the dashboard and click on "Show details" to get the list of users

4. Alternatively, view results in Finder.
    1. Go to Finder > Campaign "Teams - early adopters" > Display

results

2. Read results in the "List" view of Finder

5. After enough time is elapsed, retire the campaign.

Categorize users as Early adopters

Early adopter users can be identified in a various number of ways.

1. Categorize users as Early adopter.
    1. Create and run an investigation to select all users willing to become an Early adopter.

    2. Select all users > Click "Edit" > Select category "Teams User deployment ring" > set keyword "Early adopter" > Click on "Apply"

Get pre-deployment baseline from Early adopters

When Early adopters are defined, the second campaign "Teams - early adopters" can be sent to get baseline figures.

1. Create investigation to target recipients. In this case, users need to be categorized as "Pre-deployment" within Category "Teams User campaigns recipients".
    1. Create and run an investigation to select all users tagged as "Early adopters".
    2. Select all users > Click "Edit" > Select category "Teams User campaign recipients" > set keyword "Pre-deployment" > Click on "Apply"

2. Publish campaign
    1. The campaign already targets all users tagged with "Pre-deployment". Nothing to do here.

    2. Optionally preview the campaign

    3. Publish the campaign

3. After few days/weeks, view results in the first dashboards in the "MS Teams" module.
    1. Go to Portal > Module "MS Teams" and observe results in the "Early adopters: Satisfaction" dashboards.

    2. Track the satisfaction score and the number of "happy users" (those who answered with "Completely happy" or "Very happy").

    3. Check the Respondents ratio and Total respondents to know if you can trust the results.

4. Note: The Respondents ratio and Total respondents can vary when navigating in the hierarchy.

5. Check the distribution of the satisfaction score.

6. Check what users like and dislike the most.

4. View results in the second dashboards in the "MS Teams" module.
    1. Go to Portal > Module "MS Teams" and observe results in the "Early adopters: Adoption" dashboards.

2. Track the average number of times per week that your employees use collaboration tools, and the average number of hours per week.

3. Ensure that the Respondents ratio and Total respondents are high enough.

4. Check the distribution of the usage ? the top chart shows "How many times per week" and the bottom chart shows "How many hours" per week. (Note: the next version of the library pack will indicate this in a better way.)

5. View results in the third dashboards in the "MS Teams" module.
    1. Go to Portal > Module "MS Teams" and observe results in the "Early adopters: Collaboration" dashboards.

    2. Track the Collaboration score, both over all the population and over only those who collaborate with remote teams (this is the most important population of users).

    3. Ensure that the Respondents ratio and Total respondents are high enough.

4. Check the distribution of the preferred collaboration method.

5. Check your users' locations. Focus on those who work in different buildings or countries.

6. In addition, read what users add as comments in Finder.
    1. Go to Finder > Campaign "Teams ? pre-deployment" > Display results

    2. Read results in the "List" view of Finder.

[Optional] New users join the Early adopter programs

It can happen that new users need to be added on to the Early adopter program at any stage. If it happens, follow the steps in chapter "Categorize users as Early adopters" to categorize them as "Early adopters" in category "Teams User deployment ring". Once this is done, follow the steps in chapter "Get pre-deployment baseline from Early adopters" to categorize them as "Pre-deployment" in category "Teams User campaigns recipients". If the campaign is still published, the new users will be picked up by the investigation and be targeted with the "Pre-deployment" campaign within the next few minutes.

Deploy Teams

After enough users have replied to the ?pre-deployment? campaign, retire it and deploy Microsoft Teams to them.

Get post-deployment feedback from Early adopters

After Microsoft Teams is deployed, wait for few days/weeks before publishing the "post-deployment" campaign.

1. Create investigation to target the campaign's recipients. This time, users need to be categorized as "Post-deployment" with Category "Teams User campaigns recipients".
    1. Create and run an investigation to select all users tagged as "Early adopters".

    2. Select all users > Click "Edit" > Select category "Teams User campaign recipients" > set keyword "Post-deployment" > Click on "Apply"

2. Publish campaign
    1. The campaign already targets all users tagged with "Post-deployment". Nothing to do here.

    2. Optionally preview the campaign.

    3. Publish the campaign.

3. View results in the same three dashboards as described above "Early adopters: Satisfaction", "Early adopters: Adoption", "Early adopters: Collaboration".
4. Additionally, check the "Early Adopters: Overview" dashboard for a side-by-side overview comparison of the figures before and after the deployment of Microsoft Teams.
    1. Go to Portal > Module "MS Teams" and observe results in the "Early adopters: overview" dashboard.

2. Compare the user satisfaction pre- and post-deployment

3. Compare the user adoption (hours per week and times per week) pre-and post-deployment.

4. Compare the user collaboration score pre- and post-deployment.

5. Check on the final answer "Overall, do you think Microsoft Teams is an improvement on your previous collaboration tools?"

5. In addition, read what users add as comments in Finder.
    1. Go to Finder > Campaign "Teams ? post-deployment" > Display results

2. Read results in the "List" view of Finder.

[Optional] Staged deployment of Microsoft Teams

It can happen that all users do not get Teams installed all at the same time. If this happens, users can receive the "post-deployment" campaign in the same staged order. To achieve this, simply categorize users by batch as "Post-deployment" within category "Teams User campaigns recipients". The campaign needs to be published for the first batch and then remain published while each new batch of users get tagged.

On to Production

Following same process as described above, the same steps need to be repeated for Production users.

1. Tag users as "Production" in category "Teams User deployment ring".
2. Tag users as "Pre-deployment" in category "Teams User campaigns recipients".
3. Publish campaign "Teams - pre-deployment".
4. After few days/week, retire campaign "Teams - pre-deployment".
    1. Note: alternatively, if you wish to keep the campaign published and migrate users at the same time: When deploying Teams to a set of users, remove the tag "Pre-deployment" in category "Teams User campaigns recipients" before the migration. This will ensure they do

not receive the campaign anymore.

5. Few days/week after Teams deployed to a set of users, tag them as "Post-deployment" in category "Teams User campaigns recipients".
6. Publish campaign "Teams ? post-deployment".

Continuously monitor users' satisfaction

With Microsoft Teams deployed, this campaign asks users about their satisfaction on their last audio call. The campaign triggers automatically after a call is made, and "times out" (I.e., does not appear again to the same user) for one week. Note: the time out period can be changed in the campaign.

1. Publish campaign
    1. The campaign targets all users tagged as "Post-deployment", who makes a call. Nothing to do here.

    2. Optionally preview the campaign.

    3. Publish the campaign.

2. After few days/weeks, view results in the two corresponding dashboards in the "MS Teams" module.
    1. Go to Portal > Module "MS Teams" and observe results in the "Early adopters: Overview" or "Production: Overview" dashboards

2. Track the satisfaction score over the last 30 days

3. Track the satisfaction score over time

4. As always, make sure that the Respondents ratio and Total respondents are high enough.

Office 365 ProPlus

Office 365 ProPlus - Operate

Overview

The 'Office 365 ProPlus - Operate' pack tracks the versions of Office365 ProPlus installed on devices in your organization, the progress of channel updates to these devices, and the evolution of employees? Digital Experience and their adoption of applications over time.

When managing the production landscape, it is possible to separate machines according to multiple criteria to accurately reflect your testing environments, ensuring that proper testing of all required profiles takes place before an update arrives in production.

The pack is capable of tracking any update type, be it a new upgrade from an older version of Office to a regular channel update from Microsoft. Using category configuration, it is entirely up to the operator to decide which version(s) of Office 365 ProPlus will be tracked by the pack.

As well as tracking updates, this pack can also provide insight into the use and adoption of Office365 ProPlus. A dashboard dedicated to Employee Experience shows the relative Digital Experience scores for employees using different versions of ProPlus, as well as a breakdown of Digital Experience by individual Office applications. Similarly, an Employee Adoption dashboard uses the new Focus Time measurement to show you which individual applications are being used the most in your organization.

Pre-Requisites

The latest version of the Office365 ProPlus ? Operate pack (V2.1.0.0) is optimized for Nexthink v6.29 and later due to the use of Focus Time measurements to show Employee Adoption

The Office365 ProPlus ? Operate pack refers to Digital Experience scores in some of its dashboards therefore the Digital Experience Score pack should be installed before installing the Pack.

This pack also integrates with the Win10:Configuration pack, should you wish to

classify Business critical users or devices. Any configuration made in that pack is read by this ProPlus pack.

Change log

V2.1.0.0

Updated pack with v6.29 features, including Focus Time to measure Employee Adoption.

V2.0.0.1

Metrics have been modified to reflect Microsoft name change from ProPlus to Office365 apps

V2.0.0.0

Updated to use DEX v2

V1.0.0.1

Update ProPlus Version category

V1.0.0.0

Initial release.

Configuration

As part of the initial configuration of the pack devices can optionally be configured according to their importance to the business, which is done as part of the Win10:Configuration pack, therefore this must be imported before the Office 365 ProPlus pack and the categories for the Business and User Criticality should be configured. The remaining steps after this are for the Office 365 ProPlus pack:

1. Pre-requisite: Win10:Configuration (optional Step)
    1. Prioritizing your packages
    2. Prioritizing your device models
2. Configure Category ?ProPlus Device Ring? (optional but recommended step)

- Assign devices to the desired Rings to match your Organization's release structure. For example, if you wish to deploy to two testing rings before Production the pack comes preconfigured with Ring 0, Ring 1 and Production. If you have more (or less) testing Environments before Production you can add, remove or rename these accordingly.
- The dashboards "Create Representative Rings" and "Prioritized Devices Distribution" help you understand what your current Ring contents are, to make sure that:
    - No device is wrongly assigned to a ring (E.g., MacOS, ProPlus not installed etc)
    - No device is missing a ring (E.g., a device running Office365 ProPlus that is not in Ring 0, Ring 1 or Production)

3. Now configure the Categories "ProPlus Required Version", "ProPlus Version" and "ProPlus Unsupported Version" to reflect your desired configuration:
    - The Solution Pack is entirely flexible in terms of what versions of ProPlus you wish to monitor. By configuring these Categories you are describing which versions of ProPlus you wish to monitor:
        - ProPlus Required Version - this should contain the version number(s) you will be upgrading to. Note that any version number can be added and multiple versions can be used (for different branches). Details on ProPlus version history is published by Microsoft.
        - ProPlus Version - this should contain all the versions of ProPlus which you currently support within your Organization, configured in the same way as the above Required Version Category.
        - ProPlus Unsupported Version - This should contain versions of ProPlus that your Organization does not support.

As your Office 365 ProPlus landscape evolves you should amend these categories on a continual basis so that they accurately reflect the supported, unsupported and required versions for your Organization.

Virtualization

Virtualization: Health

Virtualization: Operate

Pre-Requisites

This pack requires some categories contained in the **Shared Categories** content pack, please make sure to have it installed in your environment before installing this pack.
The **Virtualization type** category must absolutely be configured in order to be able to target the corresponding VDI and SBC VMs. For the rest of the categories, depending on the description of each, you may or may not complete them.

Defining Excluded Applications

Configure Category **Virtualization - Excluded Applications** to list applications that will not be excluded from being reported on. This is prepopulated with a selection of common applications that would not normally be wanted. Any number of applications can be added or removed.

Defining Excluded Binaries

Configure Category **Virtualization - Excluded Binaries** to list executable that will not be excluded from being reported on. Any number of executables can be added.

Defining Back End Systems

Configure Category **Virtualization - Back End Systems** to define destinations that the Virtual Infrastructure will be communicating within your environment. This category can be individual systems or contain entire ranges as is wanted.

Defining VDI Devices

Configure Category **Virtualization type** to define the **Virtual Desktop Infrastructure (VDI)** in your environment, such as Citrix, VMWare, or Windows Virtual Desktop (WVD). This category should be assigned to all virtual machines or remote PCs that have the collector installed.

Defining SBC Servers

Configure Category **Virtualization type** to define the **Session-Based Computing (SBC)** in your environment, such as Citrix, VMWare, Microsoft Remote Desktop Server Host (RDSH) or Windows Virtual Desktop Multisession (WVD). This category should be assigned to all servers or multisession that have the collector installed.

Defining Different Virtualization Images

Configure Category **Virtualization - Virtual Image** to define the desktops that are running a particular VDI Image. This is then used for Image performance comparison within the Solution Pack. Rename the images according to needs in the category configuration.
For instance, one keyword could be named "Windows 10 VDI". Then tag your virtual machines to the keywords you just created. Here is a link to the documentation on how to tag objects with Nexthink.

Defining Infrastructure

Category **Virtualization - Operate - Infrastructure** should be completed if you install Nexthink collector on Virtual Management servers such as Citrix Director or VMware Horizon Management server.
This category is used on the **Virtualization - Operate - Controller Servers** service to monitor virtual infrastructure devices.

Defining Service and roles

Category **Virtualization - Operate - Services and roles** should be completed if you want to monitor device compliance and stability on agent

Defining Virtual Agent

Category **Virtualization - Operate - Virtual Agent** should be completed if you want to use the compliance dashboard to manage the virtual VM

compliance.

Defining VDI Network Physical / Virtual

We suggest you to adapt the network response time used in the VDI Network Physical / Virtual dashboard to measure your most important response time; for instance, the response time when connecting to a critical service in your company. To do this edit the metrics *Virtualization - Operate - Average network response time on physical devices* and *Virtualization - Operate - Average network response time on virtual devices*.

To clean the Library Pack

Please refer to the Disclaimer
Before cleaning, you can backup your **"Virtualization Operate"** Library Pack version. To backup, follow this link.

◊ **In the Finder:**

In each section described, right-click on **"Library\Virtualization Operate"** and delete.

- Services
- Metrics
- Categories
- Score

◊ **In the Portal:**

Go on the **"Virtualization Operate"** module menu then click on **"Delete Module..."**
Go on the **"Virtualization Operate Service"** module menu then click on **"Delete Module..."**

Disclaimer

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

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

Virtualization: Citrix Advanced

Summary

This pack enables the Operator to understand some important aspects of their Virtual Environment. It focuses on ensuring that the VDA Agents (where used) are correctly registered. Without this an incorrectly or malfuncitoning VDA agent can potentially take a host server offline from the perspective of managing the pool of resources which could have a direct impact on the user experience, by not allowing the user to successfully connect to their session.

It also gives visiblity on the user sentiment from the perspective of satisfaction with their experience using their virtual sessions. This important insight should be balanced with the technical metrics found in the other Virtualization packs so that a complete picture of the Digital Experience is formed.

Version

1.0.0.0 - This is the initial release of the Virtualization - Advanced Operate pack.

Pre-Requisites

This pack requires some categories which should be configured.

Upgrade Infomation

This pack does not updgrade from any other pack.

Defining SBC Servers

Configure Category **Virtualization type** that comes with the Digital Experience Score pack to define the Session Based Computing Servers in your environment, such as Citrix or Remote Desktop Services servers. This category should be assigned to all servers that have the collector installed and are SBC Server Systems.

Defining Different Virtualization Images

Once again, configure the Category **Virtualization type** but in this case, configure it to define the desktops that are running a particular VDI Image. This is then used for Image performance comparison within the Solution

Pack. Rename the images according to needs in the category configuration.
For instance, one keyword could be named "Windows 10 VDI". Then tag your virtual machines to the keywords you just created. Here is a link to the documentation on how to tag objects with Nexthink.

Remote Action Configuration

Get Citrix information

This pack uses this Remote Action in it's execution. There are no input parameters to configure for this Remote Action it should be scheduled according to frequency that you wish to run it.

Disclaimer

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

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

Virtualization Planning and Migration

Windows

Win10: Configuration

Prioritizing your packages

1. Configure Category ?Package Priority? to categorize all applications running in your environment in one of four keyword
    - 1. Business Critical - has impact on the business
    - 2. User Critical - has impact on departments, groups of people, etc.
    - 3. None - has no impact, no priority
    - 4. Out of scope - not in scope

Prioritizing your device models

1. Configure Category ?Device model Priority? to categorize all device models found in your environment in one of four keyword
    - 1. Business Critical - has impact on the business
    - 2. User Critical - has impact on departments, groups of people, etc.
    - 3. None - has no impact, no priority
    - 4. Out of scope - not in scope

Win10: Migration

Assessing software readiness

1. Pre-requisite: Win10:Configuration
    1. Prioritizing your packages

        Note: Only packages that are prioritized as "Business Critical" or "User Critical" are displayed.
2. Configure Category ?Win10 Package readiness? to categorize the applications in one of four keyword

    Ready - Can run on Windows 10
    Not Ready - Cannot run on Windows 10
    Unspecified - Compatibility with Windows 10 has not been assessed yet
    Out of scope - not in scope for migration

Assessing hardware readiness

1. Configure Category ?Win10 Device CPU readiness? to categorize the devices in one of four keywords
    Ready - CPU is ready for Windows 10
    Not Ready - CPU is not ready for Windows 10
    Insufficient data - CPU needs to be assessed manually
    Out of scope - not in scope for migration
2. Configure Category ?Win10 Device memory readiness? to categorize the devices in one of four keyword
    Ready - Device memory is ready for Windows 10
    Not Ready - Deice memory is not ready for Windows 10
    Insufficient data - Device memory needs to be assessed manually
    Out of scope - not in scope for migration
3. Configure Category ?Win10 Device graphical memory readiness? to categorize the devices in one of four keyword
    Ready - graphical memory is ready for Windows 10
    Not Ready - graphical memory is not ready for Windows 10
    Insufficient data - graphical memory needs to be assessed manually
    Out of scope - not in scope for migration
4. Configure Category ?Win10 Device disk readiness? to categorize the devices in one of four keyword
    Ready - Device has enough free space in system drive
    Not Ready - Device has not enough free space in system drive
    Insufficient data - Device free space needs to be assessed manually
    Out of scope - not in scope for migration
5. Configure Category "Win10 Device overall hardware readiness? to categorize the devices in one of four keyword
    Ready - Device hardware is ready for Windows 10
    Not Ready - Device hardware is not ready for Windows 10
    Insufficient data - Device hardware needs to be manually assessed
    Out of scope - not in scope for migration

Monitoring migration progress

1. Pre-requisite: Install & configure Digital Experience Score
2. Configure Category "Win10 Device migration? to categorize the devices in one of 3 keyword
    1. To migrate - Devices not yet running Windows 10
    2. Migrated - devices running Windows 10
    Out of scope - devices not in scope for migration

Win10: Feature Update

Creating representative rings for feature updates

1. Pre-requisite: Win10:Configuration
    1. Prioritizing your packages
    2. Prioritizing your device models
2. Configure Category ?Win10 Device ring for feature update?

The dashboard "Create representative rings" helps you to make sure that

- No device is wrongly assigned to a ring (E.g., MacOS, Server, etc)
- No device is missing a ring (E.g., a Windows 10 device that is not in Ring 0, Ring 1 or Production)
- No device is assigned twice (E.g., a device that is in Ring 0 for the Quality update and Ring 1 for the Feature update. A device that is assigned in Ring 0 in Quality update must be in Production for the Feature update, etc.)

Migrating and monitoring the next Feature update version

1. Pre-requisite: Create representative rings for feature update
2. Pre-requisite: Install & configure Digital Experience Score
3. Configure Category ?Win10 Feature update target build? with the target build numbers of Windows 10.

Win10: Quality Update

Creating representative rings for quality updates

1. Pre-requisite: Win10:Configuration
    1. Prioritizing your packages
    2. Prioritizing your device models
2. Configure Category ?Win10 Device ring for quality update?

The dashboard "Create representative rings" helps you to make sure that

- No device is wrongly assigned to a ring (E.g., MacOS, Server, etc)
- No device is missing a ring (E.g., a Windows 10 device that is not in Ring 0, Ring 1 or Production)

- No device is assigned twice (E.g., a device that is in Ring 0 for the Quality update and Ring 1 for the Feature update. A device that is assigned in Ring 0 in Quality update must be in Production for the Feature update, etc.)

Migrating and monitoring the next Quality update version

1. Pre-requisite: Create representative rings for feature update
2. Pre-requisite: Install & configure Digital Experience Score
3. Configure Category ?Win10 Quality update target build? with the target build numbers for each versions of Windows present in your environment.

Windows Defender Management

Overview

The Windows Defender Management library pack gives an understanding of the Windows Defender landscape. The core points of Windows Defender are that both the Engine and Signature files are up to date and that scans are regularly running and the pack delivers this knowledge.

There are two dashboards to use. The first, **Overview** gives an understanding of the landscape compliance in terms of engine versions and Defender functionality enabled.

The second, **Signatures and Scans** ensures that the software is up to date from a antivirus signature and scanning perspective.

Pre-requisites

The pack should be imported into the Nexthink environment. If you have the existing Defender Pack installed please choose **Replace** for any of the Remote Actions and metrics so that the new ones are in force. Note of course as usual any customizations you have made to the existing metrics before an import should be reapplied post import.

Configure the protection level

By configuring the protection level you will be able to focus on the level of protection that matters for you.

You can update the protection level with the **following steps**:

1. On the finder, edit the metric: "WinDefender - Devices with any protection disabled"
2. Delete unwished protection levels, and it will not be taken into account:

    - Antivirus enabled
    - AntiSpyware enabled
    - Behavior Monitor enabled
    - Ioav protection enabled
    - NIS enabled
    - On access protection enabled

Configure RA execution frequency

You can set an investigation to execute the RA automatically.

To do so, you can **follow the steps below** on the Finder:

1. Navigate to the On-demand remote action folder.
2. Edit the "Get Windows Defender Information" remote action.
3. Tick "Automatically run the remote action".
4. if needed, modify the the investigation execution frequency (default value is every 1h).

Configure the Remote Worker Category

One of the views common in the library pack is viewing various activities by worker type, i.e. whether these are Office workers or Remote workers. This category is common across a number of Nexthink library packs and first appeared in the Remote Worker pack.

Should you have the Remote Worker pack installed, you will already have configured this category and so no further action is needed. If you have not configured this, then please configure your **Remote Worker vs Office Worker Device** category using these instructions

Administrators Management

Pack configuration

Administrators Management:

1. **Optional Configuration**
   Two possible optional Nexthink Categories in this pack:
2. **Pilots Categories**
   There is no limit to what can be configured. It is perfectly reasonable to remove any of the above or add any that are wished for.
   - **AdministratorsManagement - Administrators Whitelist**

   This Category determines the AdministratorsManagement whitelist. This can be used to exclude administrators from the metrics except for external/web/mail traffic.
   It will help you to detect unauthorized admin

   - **AdministratorsManagement - Destinations tagging**

   This Category determines the mail/proxy network fqdn.
   It will help you to limit the risk of administrator exposure on the Internet to prevent serious infections.

3. **To clean the Library Pack:**
   Before cleaning, you can backup your **"AdministratorsManagement"** Library Pack version. To backup, follow this link.
   - **In the Finder:**

   In each section described, right-click on **"Library\AdministratorsManagement"** and Delete.
     - Metrics
     - Categories
   - **In the Portal:**

   Go on the **"AdministratorsManagement"** module menu then click on **"Delete Module..."**

Webex

Webex Operate

Overview

This pack gives an overall view of devices running Webex to help you get a status of the landscape. Please note that this view is different from the statistics available in the Webex Cloud. It gives you information on usage on Windows devices.

Understand Webex applications & executables

1. ptoneclk.exe
    - This executable is the main Webex Desktop Client. It is monitored to track devices running Webex and not necessarily performing audio or video calls.
1. atmgr.exe and webexmta.exe
    - Either of these executables is run when Webex meetings are launched.

Pre-Requisites

- This pack has no mandatory pre-requisites and can be run directly without configuration. However optional configuration may be necessary as described below.

Understand Webex application

Application Cisco Webex Meeting

- Used as a ?catch-all? filter in the version dispersion metrics to display any executable related to Webex.

Device category "Remote Worker vs Office Worker Device"

- This category is used by multiple library pack. Please go to its dedicated configuration page for more information about it.

Domain category "Webex Domains"

- This category holds all domains that Webex uses during normal operations. The associated metric reports on the data volumes going to them.

Executable category "Webex "

- This category lists all executables used by the Webex suite. The associated metrics reports on overall application stability and response time.

Change log

V1.1.0.0

Fixed metrics wrongly referencing to Zoom

V1.0.0.1

Fixed the description

V1.0.0.0

The initial release of the Webex Operate library pack.

Zoom

Zoom Operate

Device category "Remote Worker vs Office Worker Device"

This category is used by multiple library pack. Please go to its dedicated configuration page for more information about it.

Remote Actions

Get Performance Monitor Data

Overview

With this Remote Action, execute Data Collector Sets and move the reports to a desired shared folder.

Prerequisites

There is not any special requirement to use this Remote Action. It is possible to configure your custom Data Collector Set, otherwise *System Performance* is used as the default one.

To better understand how to configure a shared folder to work with Nexthink Act, please visit this page.

Custom Data Collector Set

To customize your own Data Collector Set, please, have a look at this link.

The XML scheme needs to be available in a shared folder to be used by the Remote Action.

Execution context

The Remote Action must be executed as LocalSystem, in order to have the right of executing Performance Monitor analysis.

Input parameters

To a good usage of the Remote Action, set these input parameter values:

Parameter	Description	Value
MaximumDelayInSeconds	To avoid overloading the network when saving the reports	30
XMLPath	"" to execute the default Data Collector Set called *System Performance* or an UNC path to	""

	the configured XML scheme	
OutputFolderPath	UNC path where the reports will be exported	eg. \\server\folder

Restart Device

Overview

Tests if a restart is necessary due to too long device uptime, or pending patch installation, and based on provided input configures restart of the target device. The campaign is displayed to enable user immediate restart or postpone until the next script execution. After the restart, previously opened user's applications are restored.

Input parameters

Parameter	Description	Value
TestPendingRestart	Controls if the script should verify if the device is pending restart due to recently installed patch. A positive result will lead to trying to restart the device following the options selected on the other inputs.	• Valid values: True/False • Default: True
CampaignId	Campaign GUID asking the end-user for restart. The end-user needs to respond NOW to trigger the restart. If not, the restart is postponed.	• Empty string ("") or empty GUID (00000000-0000-0000-0000-000000000000) are valid values only if ShowCampaign input is filled with "Never". • Default: 4fc67441-e4e3-4905-b533-620eb4083c2b
ShowCampaign	Determines circumstances the campaign is displayed to the end-user. The campaign will give the end-user the	• Valid values are: ♦ Always: Campaign is displayed to end-user at every remote action execution and device restart is never forced.

	option to postpone the restart or execute it now.	♦ DuringGracePeriod: End-user will have a limited time to postpone device restart. When the grace period expires, a forced restart is executed. The length of the grace period is provided in PostponeGracePeriodInDays input parameter. ♦ OnlyFirstExecution: End-user is notified via the campaign only the first time the remote action is executed. When the remote action is executed a second time the restart will be forced. ♦ Never: The end-user is never asked. The restart is always force. • Default: Always
NumberOfDaysSinceLastReboot	Maximum number of days allowed for the device to be running without a restart. A day is 24 hours therefore, forced restart is triggered only if the remote action detects that end-user postponed restarting more than 24 hours ago.	• Range: 1-60. • Default: 30
PostponeGracePeriodInDays	Maximum number of days that end-user can postpone restart when ShowCampaign is DuringGracePeriod. This input will only take effect if the remote action is executed more than once.	• Range: 1-30. • Default: 7

RestartDelayInSeconds	Delay time between initiating restart and it's execution if restart conditions have been met.	• Range: 45-86400. • Default: 300

Recommendations

Recommended timeout: 720 Recommended way of use: Schedule the remote action to be executed once per day.

IMPORTANT: If you don't execute the RA periodically, PostponeGracePeriodInDays won't work as designed.

Common use cases

I want to keep the company devices restarted at least once each 15 days but I don't want to do it without the consent of the end-user

Recommended Inputs

- TestPendingRestart: **false**
- CampaignId: **4fc67441-e4e3-4905-b533-620eb4083c2b**
- ShowCampaign: **Always**
- NumberOfDaysSinceLastReboot: **15**
- PostponeGracePeriodInDays: **7** (this value won't affect the execution but needs to be an integer between 1 and 30)
- RestartDelayInSeconds: **300**

I want to enforce that the company devices have the latest Windows patch or restart devices that have been running more than 30 days. I want to let the end-user 3 days to restart in their own terms but if they don't, force the restart either way.

Recommended Inputs

- TestPendingRestart: **true**
- CampaignId: **4fc67441-e4e3-4905-b533-620eb4083c2b**
- ShowCampaign: **DuringGracePeriod**
- NumberOfDaysSinceLastReboot: **30**
- PostponeGracePeriodInDays: **3**
- RestartDelayInSeconds: **300**

I want the company devices to be restarted when their uptime is bigger than a week or when they have pending Windows patches. I want to ask one time but if they ignore the notification, the restart should be forced.

Recommended Inputs

- TestPendingRestart: **true**
- CampaignId: **4fc67441-e4e3-4905-b533-620eb4083c2b**
- ShowCampaign: **OnlyFirstExecution**
- NumberOfDaysSinceLastReboot: **7**
- PostponeGracePeriodInDays: **7** (this value won't affect the execution but needs to be an integer between 1 and 30)
- RestartDelayInSeconds: **300**

Other values

End-user execution: Current interactive user

Compatibility: Windows 10 and Windows 7