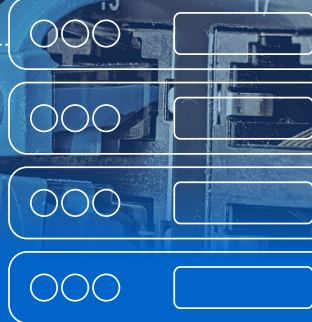


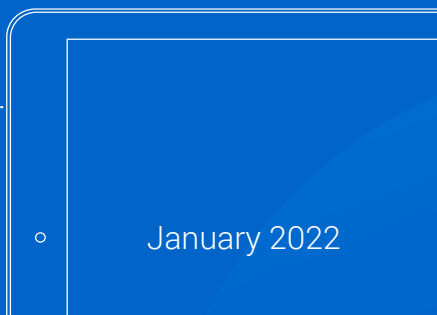


TeamViewer
Remote Management



TeamViewer Remote Management User Guide

Monitoring & Asset Management
Endpoint Protection
Backup
Web Monitoring



January 2022

Table of Contents

1. General	5
1.1. About the User Guide	5
1.2. About TeamViewer Remote Management	5
2. Requirements	7
2.1. Licensing	7
2.2. License Activation	8
2.3. System Requirements	9
2.3.1. TeamViewer Monitoring & Asset Management	9
3. Get Started	10
3.1. Activation	11
3.1.1. TeamViewer Full Version Activation	11
3.1.2. Management Console Activation	14
3.2. Policies	16
3.2.1. Default Policy and Policy Options	17
3.2.2. Assign a Policy	18
4. Monitoring & Asset Management	19
4.1. Monitoring & Asset Management Activation	20
4.2. Monitoring Checks	20
4.3. Monitoring Policy	28
4.4. Remote Task Manager	28
4.5. Alarms and Notifications	29
4.5.1. Alarms	29
4.5.2. Notifications	30
4.6. Monitoring Device View	31
4.7. Monitoring Alarms View	32
4.7.1. Monitoring Filtering	33
4.7.2. Monitoring Export	34
4.8. Network Monitoring	34
4.8.1. Network Monitoring Activation	35
4.8.2. Network Monitoring Settings	36
4.8.3. Network Monitoring Checks	36
4.8.4. Network Monitoring Policy	37
4.8.5. Network Monitoring Views	38
4.9. Remote Scripting	39
4.10. Monitoring API	43
4.10.1. Monitoring API actions	43
4.11. Asset Management	44
4.11.1. Device View	44
4.11.2. Asset View	46
4.11.3. Patch View	48
4.11.4. Patch Management Policy	49
4.11.5. Software Deployment	51

4.12.	<i>Software Deployment History Logs</i>	58
4.13.	<i>Asset and Patch Management API</i>	59
5.	Endpoint Protection and Endpoint Detection and Response – powered by Malwarebytes	60
5.1.	<i>Requirements</i>	60
5.1.1.	Operating System requirements for Malwarebytes Endpoint Protection.....	60
5.1.2.	Operating System requirements for Malwarebytes Endpoint Detection and Response	60
5.1.3.	Windows hardware requirements.....	60
5.1.4.	Apple hardware supported	60
5.1.5.	Operating system annotations	60
5.1.6.	Network access and Firewall settings requirements.....	61
5.2.	<i>Licensing</i>	61
5.2.1.	Activation.....	62
5.3.	<i>Product pages and views</i>	63
5.3.1.	Dashboard view	63
5.3.2.	Devices View	64
5.3.3.	Detection View	66
5.3.4.	Suspicious Activity View	67
5.4.	<i>User Management</i>	69
5.4.1.	User Roles.....	69
5.5.	<i>Group Management</i>	71
5.6.	<i>Policies</i>	71
5.6.1.	Settings available in the TeamViewer Management Console	72
5.6.2.	Settings available in Endpoint Detection and Response	75
5.6.3.	Settings available in the Malwarebytes Nebula	76
5.7.	<i>Scan Schedules</i>	77
5.7.1.	Threat Scans	77
5.7.2.	Hyper Scans	77
5.7.3.	Custom Scans.....	77
5.8.	<i>Exclusions</i>	78
5.8.1.	Exclusion Types.....	79
5.8.2.	Protection layers.....	80
5.9.	<i>Quarantine</i>	81
5.10.	<i>Notifications</i>	82
5.10.1.	Configuration.....	82
6.	Endpoint Protection – powered by Bitdefender (Legacy solution)	84
6.1.	<i>Activation</i>	84
6.2.	<i>Policies</i>	84
6.2.1.	Settings	85
6.2.2.	Exclusions	86
6.2.3.	Notifications	86
6.3.	<i>Dashboard</i>	87
6.3.1.	Manage Endpoints.....	87
6.3.2.	Manage Policies.....	88
6.3.3.	Manual Scans.....	88
6.3.4.	Status of the Device.....	88
6.3.5.	Quarantine.....	89
6.3.6.	Active Ransomware Protection	89
6.3.7.	Device View	89

6.3.8.	Threat View	91
7.	Backup	93
7.1.	<i>Backup Activation</i>	94
7.2.	<i>Policies</i>	94
7.2.1.	Policy Name	95
7.2.2.	Add a Backup Policy	95
7.2.3.	File Selection.....	95
7.2.4.	Backup Settings	96
7.2.5.	Schedule Backup.....	97
7.2.6.	Bandwidth Throttling.....	97
7.2.7.	Exclusion.....	97
7.2.8.	Notifications	98
7.3.	<i>Retention Period</i>	98
7.4.	<i>Manage Backup</i>	99
7.4.1.	Backup Status	99
7.4.2.	Status Description.....	100
7.4.3.	Daily Storage Usage Per Device	101
7.4.4.	Delete Files from Backup	101
7.5.	<i>Restore Backed Up Files</i>	102
7.5.1.	Restore to the Original Device.....	102
7.5.2.	Restore to Another Device	102
7.5.3.	Restore from Previous Backup	102
7.6.	<i>File Selection for Restore</i>	103
7.7.	<i>Backup Device View</i>	105
7.7.1.	Filtering.....	105
7.7.2.	Storage Used Overview	105
8.	Web Monitoring.....	106
8.1.	<i>Web Monitoring Activation</i>	106
8.2.	<i>Web Monitoring monitor types</i>	106
8.2.1.	Uptime monitors	106
8.2.2.	Page Load monitors.....	108
8.2.3.	Transaction monitors.....	108
8.2.4.	Monitors configurations set up	109
8.2.5.	Transaction Recorder plugin installation.....	113
8.2.6.	Transaction Scripts recording	114
8.2.7.	Transaction recorder used commands list	120
8.3.	<i>Monitors data visualization</i>	127
8.4.	<i>Alarms, Notifications and Error types</i>	135
8.4.1.	Alarms.....	135
8.4.2.	Notifications	137
8.4.3.	Error types	138
8.5.	<i>Monitor Collections and User Management</i>	140
8.5.1.	Monitor Collections	140
8.5.2.	User Management.....	141
8.5.3.	Sharing Monitor Collections	142
8.6.	<i>Data exporting</i>	143
8.7.	<i>Web Monitoring API</i>	143
8.7.1.	Web Monitoring - API Actions	143

9.	Contact book and Integrations.....	144
9.1.	<i>TeamViewer Contacts.....</i>	<i>145</i>
9.2.	<i>External Contacts</i>	<i>146</i>
9.3.	<i>Contact groups</i>	<i>147</i>
9.4.	<i>Integrations.....</i>	<i>149</i>
9.4.1.	<i>Webhook</i>	<i>149</i>
10.	Reporting	153
10.1.	<i>Web Monitoring reports.....</i>	<i>153</i>
11.	Support.....	155

1. General

1.1. About the User Guide

This user guide describes how to work with the Remote Management tool from TeamViewer. Unless stated otherwise, the functionalities described always refer to the TeamViewer full version for Microsoft Windows. Mac OS, iPhone, and iPad are trademarks of Apple Inc. Linux® is a registered trademark of Linus Torvalds in the US and other countries. Android is a trademark of Google Inc. Windows and Microsoft are registered trademarks of Microsoft Corporation in the US and other countries. For simplification purposes, this manual refers to the operating systems Microsoft® Windows® XP, Microsoft® Windows® Vista, Microsoft® Windows® 7, Microsoft® Windows® 8 and Microsoft® Windows® 10 simply as “Windows.” For a list of all supported operating systems, visit our [website](#) or our [Community](#) page to learn more.

1.2. About TeamViewer Remote Management

TeamViewer Remote Management is a professional and efficient IT management platform integrated into a secure remote desktop access tool, completely tailored to your company's needs. The platform is designed to protect and remotely monitor devices, to keep track of IT assets, and/or to store the data in a secure cloud backup. In order to achieve these goals, TeamViewer Remote Management offers the following services, available on the TeamViewer Management Console and on the TeamViewer client:

TeamViewer Monitoring & Asset Management

TeamViewer Endpoint Protection

TeamViewer Backup

TeamViewer Web Monitoring

With TeamViewer Remote Management, you will maintain a clear overview of all the important information and functions of your system and IT infrastructure.

1. With **TeamViewer Monitoring & Asset Management**, you can proactively monitor your devices, and set up individual checks to receive notifications on, for example, disk health, antivirus software, online status, RAM use, and running processes on a computer. The integrated Asset Management feature also lets you track your deployed assets and create IT inventory reports for your network. Manage all your devices conveniently via the TeamViewer Management Console or your TeamViewer Client and receive direct e-mail alerts.

2. With **TeamViewer Endpoint Protection**, you can keep your computers clean and safe. Endpoint Protection safeguards your devices against threats such as viruses, Trojans, rootkits, and spyware, 24/7 - no matter if on- or offline. Endpoint Protection scans your devices on a regular basis, discovers potential threats early, and protects your devices reliably. Discovered malware is terminated immediately and can later be completely deleted. With the TeamViewer Management Console, you can manage all threats and scans at a glance – anytime, anywhere.
3. With **TeamViewer Backup**, you can store your data in the cloud under the highest security standards, and backed up files can be remotely restored from anywhere, at any time. Protect your important files by backing up the complete file system, common file formats, or specific files and folders regularly. Restore files and thus avoid potential data loss. With the TeamViewer Management Console, you have access to each backup of any of your devices at any time.
4. With **TeamViewer Web Monitoring**, you can check the availability and response times of your website. Our globally distributed servers will check your website regularly and will inform you if your page is down or is taking too long to respond. Get insight into the load times of your page, and immediately see which elements on your website cause a higher load, so you can optimize your end user experience. You can also script crucial transactions on your website and run them automatically on a regular basis and be alerted if a transaction fails to understand if your web shop is running smoothly or your customer login is working properly.

2. Requirements

These are the requirements that must be met in order to use all the functions of TeamViewer Remote Management.

Note: You can also try TeamViewer Remote Management free for 14 days, with no license or obligation to subscribe.

2.1. Licensing

TeamViewer Remote Management is an add-on to the TeamViewer remote control product, but it is not included in the TeamViewer license model. This means that:

1. Remote Management is not part of the TeamViewer Corporate, Premium, or Business license.
2. Remote Management can be used even without a TeamViewer Corporate, Premium, or Business license.
3. You'll need a TeamViewer Remote Management license in order to use all the functions of Remote Management.

TeamViewer Remote Management services are available as a monthly or an annual subscription. Under the Remote Management license model, you purchase a so-called "endpoint" for each computer you want to use Remote Management on. The Backup license counts the storage volume. The Web Monitoring license is based on packages that include variables such as types and number of monitors, check frequency and the number of locations you want your monitors to run from.

Note: You will need separate endpoints for the TeamViewer Remote Management services: Monitoring & Asset Management and Endpoint Protection. The different endpoints can be used independently of one another.

For example:

1. If you want to protect five (5) computers with TeamViewer Endpoint Protection, you'll need a TeamViewer Endpoint Protection license with 5 endpoints.
2. If you want to monitor ten (10) computers with TeamViewer Monitoring & Asset Management, you will need a TeamViewer Monitoring & Asset Management license with 10 endpoints.
3. If you want to backup twenty (20) computers with TeamViewer Backup, you will need a TeamViewer Backup license with the necessary storage volume. TeamViewer Backup can be installed on unlimited devices.

Note: The licensing for the Backup service is based on the consolidated storage volume used. Therefore, the service can be used on an unlimited number of endpoints.

4. If you want to have 20 basic and 10 advanced monitors with 5 and 20 minutes check frequency respectively, from 3 out of 30 locations maximum, then you need to buy a custom package, but if you only want to have 50 basic monitors, you can purchase a Basic package

For more information about the Remote Management license model, visit our [TeamViewer Remote Management shop](#).

2.2. License Activation

You need a TeamViewer Remote Management license in order to use all the functions of the TeamViewer Remote Management services.

After you purchase a TeamViewer Remote Management license, you'll receive a confirmation e-mail. Click on the activation link in the e-mail in order to activate the license for your TeamViewer account.

Once you have activated the license, it will automatically be linked to your TeamViewer account and will be ready for immediate use.

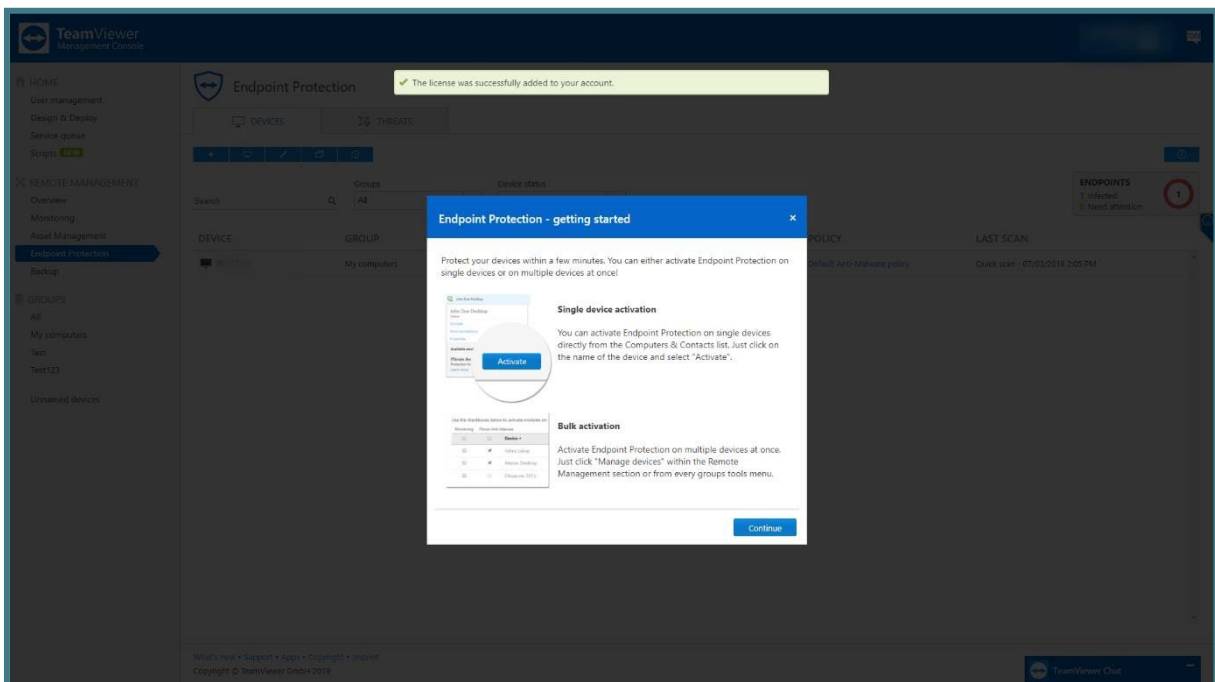


Image: Remote Management license activation.

Note: If you set up your TeamViewer account under a company profile, the TeamViewer Remote Management license will be part of the company profile and all users with permission will be able to manage the Remote Management services.

Note: TeamViewer Remote Management license activations can only be undone in exceptional cases.

Note: Only one TeamViewer Web Monitoring license can be activated per account.

2.3. System Requirements

To configure and manage TeamViewer Remote Management services, you will need the TeamViewer Management Console.

The TeamViewer Management Console is browser-based and is therefore independent of the operating system.

To activate and to view alerts, you can use the TeamViewer full version with the following operating systems:

4. Windows

To view alerts only you can install the TeamViewer remote control application on:

1. Android
2. iOS

2.3.1. TeamViewer Monitoring & Asset Management

To use Monitoring, one of the following operating systems must be running on the devices (endpoints) you wish to monitor:

Windows

1. Windows 10 / 8.1 / 8 / 7 (Windows 7: By default, only TLS1.0 is enabled on Windows 7. Due to security concerns, connections to TeamViewer servers are now only possible with at least TLS1.2.)
2. Windows Server 2022 / 2019 / 2016 / 2012 R2 / 2012 / 2008 R2 / 2008
3. The antivirus software check is not available for server operating systems.
 - o Windows Security Center (WSC) is not active on Windows Service OS.
4. TeamViewer 11 full version of Host (or newer) must be installed.

macOS

1. macOS 10.12 (Sierra), (10.13) High Sierra, 10.14 (Mojave), 11.2-5 (Big Sur), 12 (Monterey)

2. TeamViewer 14 full version of Host (v14.2.2558 and newer)
 - a. TeamViewer needs to start with the systemstartup

Linux

1. Debian 9 or newer
2. GRML, Kali Linux, Purism, Pure OS, Tails, Ubuntu and other .deb distributions.
3. TeamViewer 14 full version of Host (14.1.9025 and newer).
 - a. Account needs to be assigned before activation.

To use Asset Management (which includes Patch Management), one of the following operating systems must be running on the devices (endpoints) you wish to monitor:

- Works with the latest version of TeamViewer 14 (14.5.1691) and newer.
- Only compatible with these Windows Operating systems
 - o Windows 7 SP1/8.0/8.1/10
 - o WindowsServer2008R2/2012/2019

2.3.2. TeamViewer Endpoint Protection

To use Endpoint Protection, one of the following operating systems must be running on the devices (endpoints) you wish to protect:

1. Windows 10 / 8.1 / 8 / 7.
2. Windows Server 2012 R2 / 2012 / 2008 R2.
3. TeamViewer 11 full version or Host (or newer) must be installed.

2.3.3. TeamViewer Backup

To use Backup, you should make sure that one of the following operating systems is running on the device(s) you wish to backup using TeamViewer Backup:

- Windows 10 / 8.1 / 8 / 7 SP1 and later.
- Windows Server 2012 R2 / 2012 / 2008 R2.
- TeamViewer 11 full version or Host (or newer) must be installed.

3. Get Started

You can use the TeamViewer Management Console to configure all Remote Management services. To do this, open the TeamViewer Management Console at <https://login.teamviewer.com> and log in with your TeamViewer account. All other steps for configuring TeamViewer Remote Management are described below.

Note: Depending on user permissions, TeamViewer accounts set up under a company profile can also use the functions described below.

3.1. Activation

All computers that users want to use TeamViewer Remote Management on are called “endpoints.” The TeamViewer Remote Management service must be activated and configured on each endpoint. The license can be activated using bulk activation or on each endpoint separately.

After activating **Monitoring & Asset Management** on the endpoints, the following steps are taken automatically:

1. The **Monitoring** service is downloaded and installed on the device.
2. The Asset Management service, which is also responsible for Patch Management is downloaded and installed on the device
3. The default **Monitoring & Asset Management** policy is assigned to the device.
4. Asset Management data is uploaded for the first time.
5. The information of missing patches is uploaded for the first time.

After activating **Endpoint Protection** on the endpoints, the following steps are taken automatically:

1. The **Endpoint Protection** service is downloaded and installed on the device.
2. The latest **Endpoint Protection** virus definitions are downloaded.
3. The **Default Endpoint Protection policy** is assigned to the device.
4. A Quick scan is started.

After activating **Backup** on the endpoints, the following steps are taken automatically:

1. The **Backup** service is downloaded and installed on the device.
2. You must define a default Backup policy with file paths to backup.

After activating **Web Monitoring** you can start creating and configuring you monitors.

Note: For Transaction Monitoring you also need to download and add the Browser plugin (Transaction Recorder) as an extension– please see: [Transaction recorder plugin installation](#)

3.1.1. TeamViewer Full Version Activation

Single Activation

You can activate Remote Management services* for individual devices on your Computers & Contacts list. First, the device is assigned to your TeamViewer account and then the Remote Management service is configured.

*When **Monitoring & Asset Management** is activated directly from a device **Patch Management** will not be activated. This can only be activated from the TeamViewer Management Console.

To do this:

- 1) Click the device name in your Computers & Contacts list.
- 2) Select Activate for the respective service.

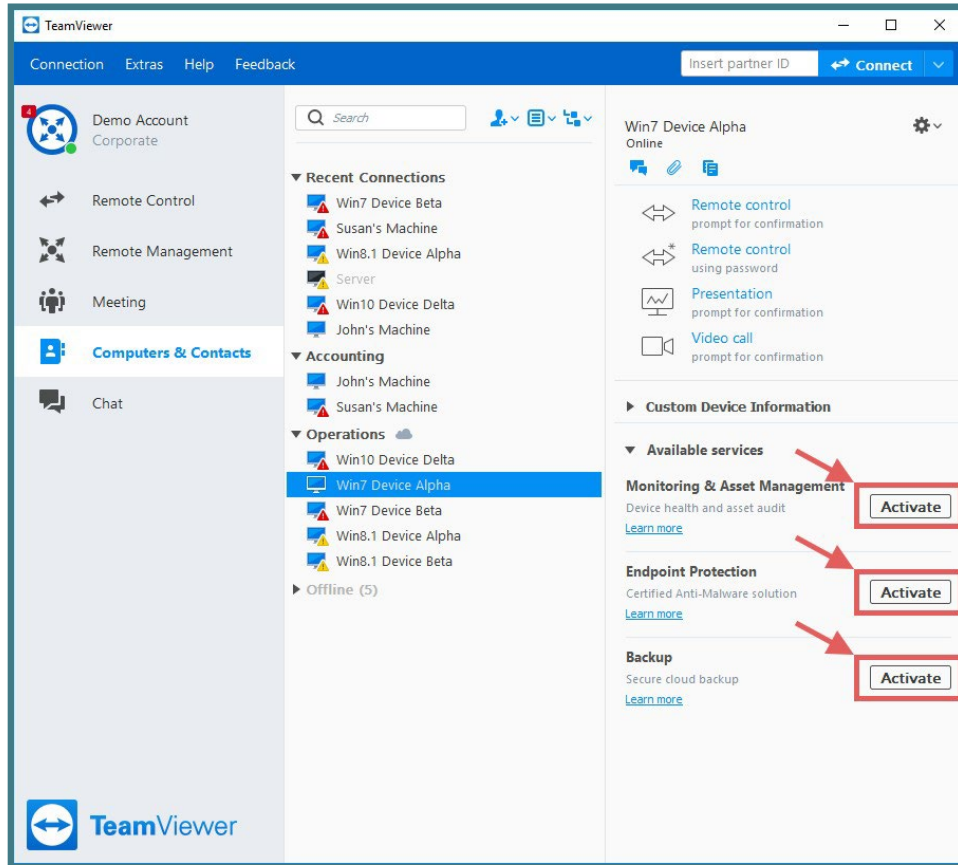


Image: Activation via TeamViewer full version.

If you haven't saved the personal password for the device in your Computers & Contacts list, enter it in the dialog box.

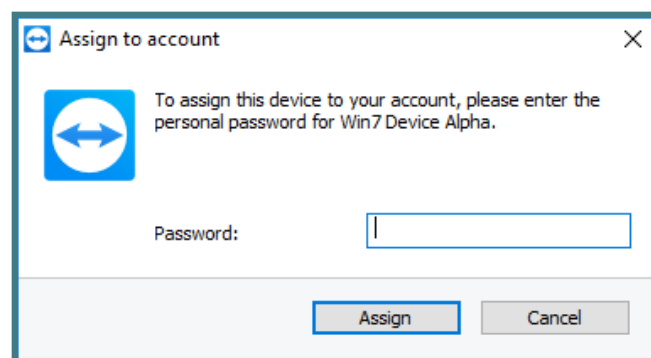


Image: Device account assignment.

If you have not set a personal password for the endpoint, you can assign the endpoint to your account via the settings in the TeamViewer full version.

To do so, you'll need to access the settings locally on the computer under:

Extras → Options → General → Account assignment.

Remote Management Tab

Starting with TeamViewer 14 and up, we introduced a new tab in the TeamViewer client.

Remote Management Tab will display the status for all active services, and will contain quick links to the Management Console:

1. Activate an endpoint button



2. Open Settings

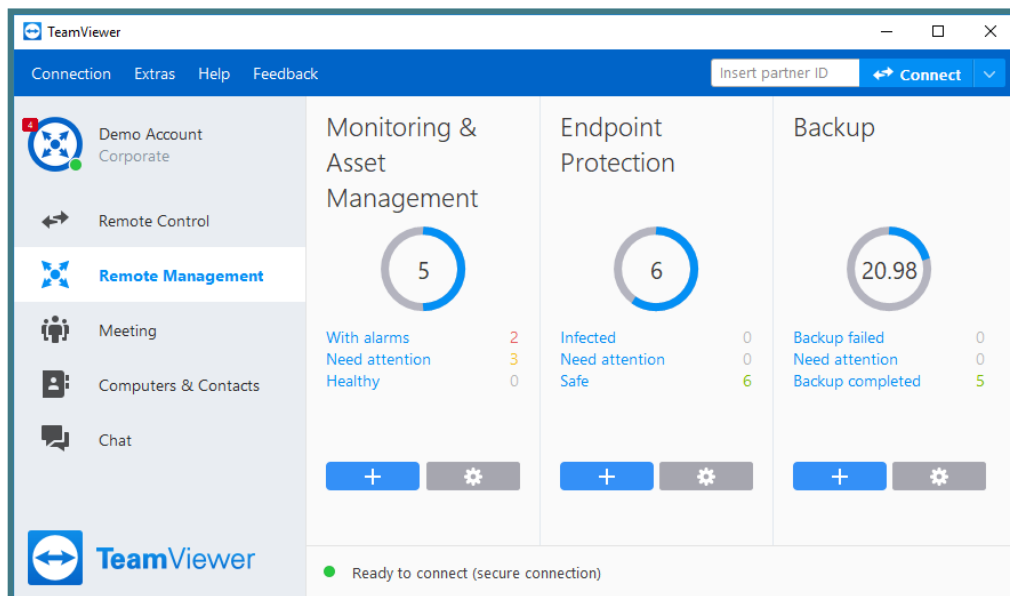


Image: Remote Management tab in the TeamViewer client.

3.1.2. Management Console Activation

TeamViewer Management Console can be accessed here: <https://login.teamviewer.com>

Single activation

You can activate Remote Management services for individual devices in your Groups list. In order to use this feature, you must have an active license.

1. Go to any group in the left pane, select the device, and click on the desired services icon on the right side.
2. Click activate.
3. Now, the device is assigned to your TeamViewer account, and then the respective Remote Management service is configured.

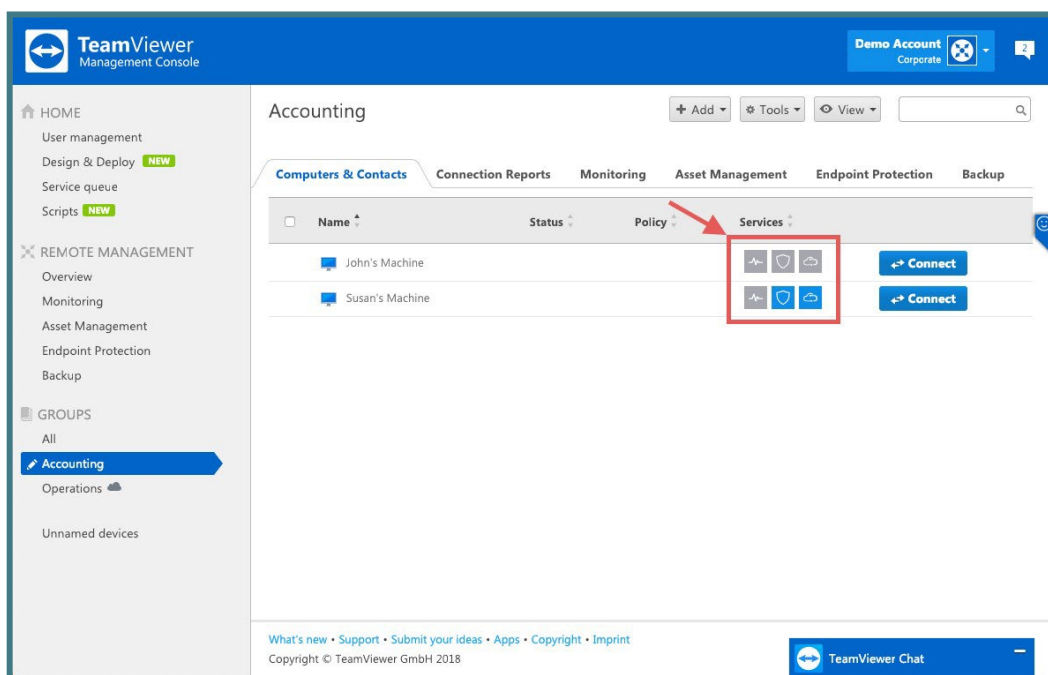


Image: Single activation via TeamViewer MCO.

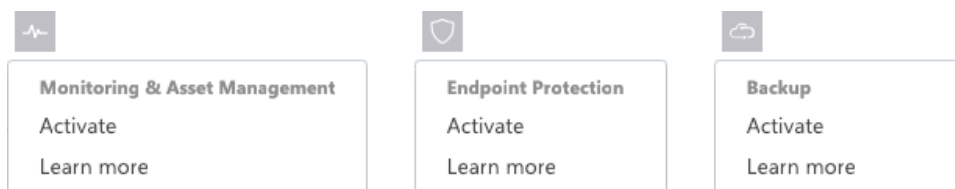


Image: Activation icons.

Bulk activation

Bulk activation helps you activate TeamViewer Remote Management services on multiple devices and assigns all of them to your TeamViewer account collectively. By using your personal passwords, all endpoints are automatically assigned to your account and the TeamViewer Remote Management service(s) will be activated for the endpoints in one step. In order to use this feature, you must have an active license.

1. Activate from Remote Management overview.
 - a. Click on the 'Overview' tab under Remote Management section on the left pane.
 - b. Click on the '+' button from the lower left corner of the service tile.
 - c. Select the devices from the list and click next.
 - d. Select the default policy that should be assigned for all devices.
 - e. Click activate.

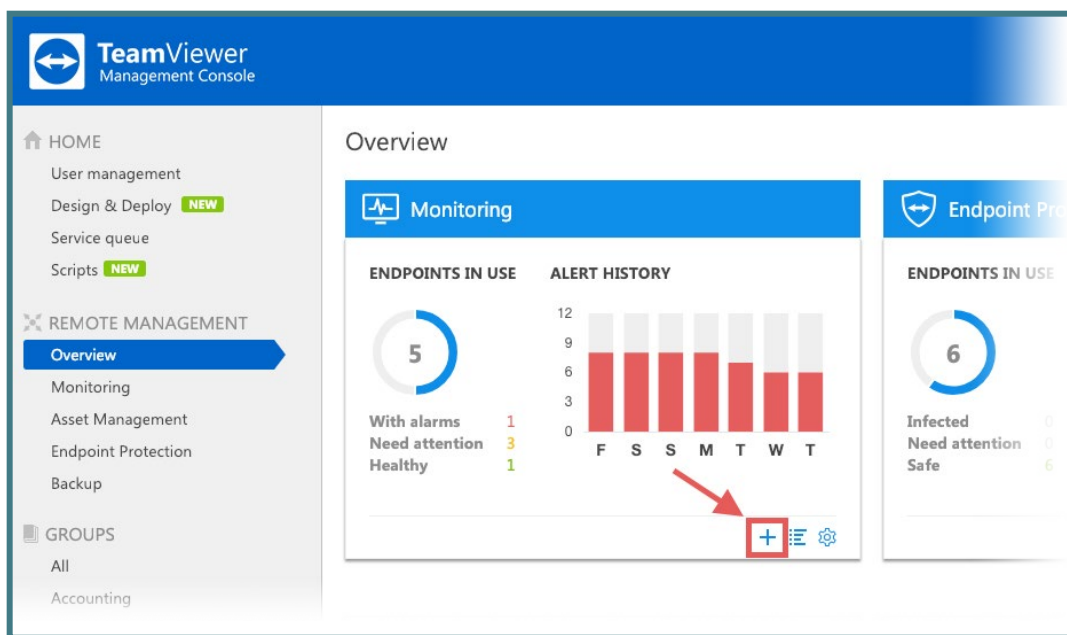


Image: Bulk activation via TeamViewer MCO 1.

2. Activate from the service tab.
 - a. Click on the service tab you want to activate endpoints for.
 - b. Click on the '+' button on the upper left corner.
 - c. Select the devices from the list and click next.
 - d. Select the default policy that should be assigned for all devices.
 - e. Click activate.

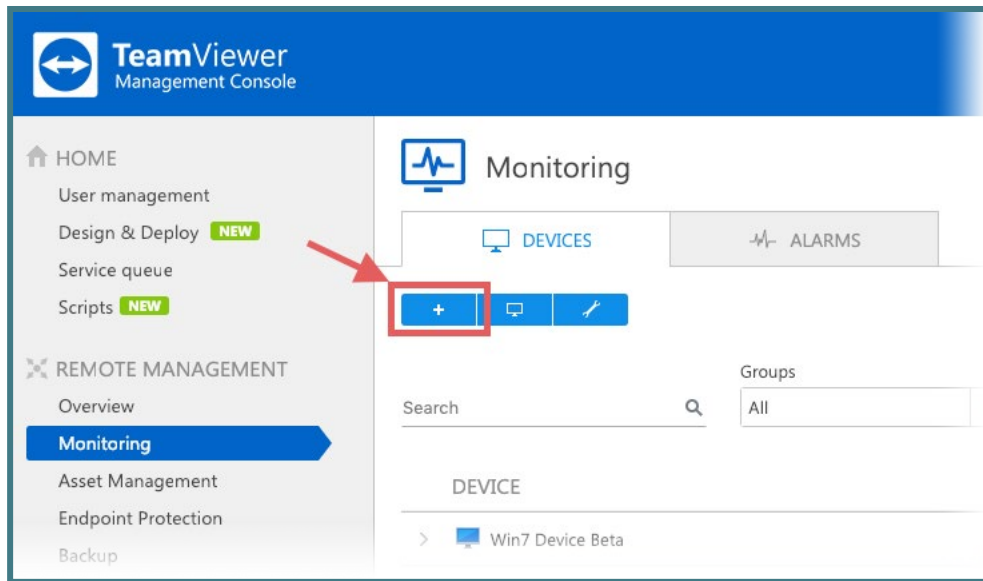


Image: Bulk activation via TeamViewer MCO 2.

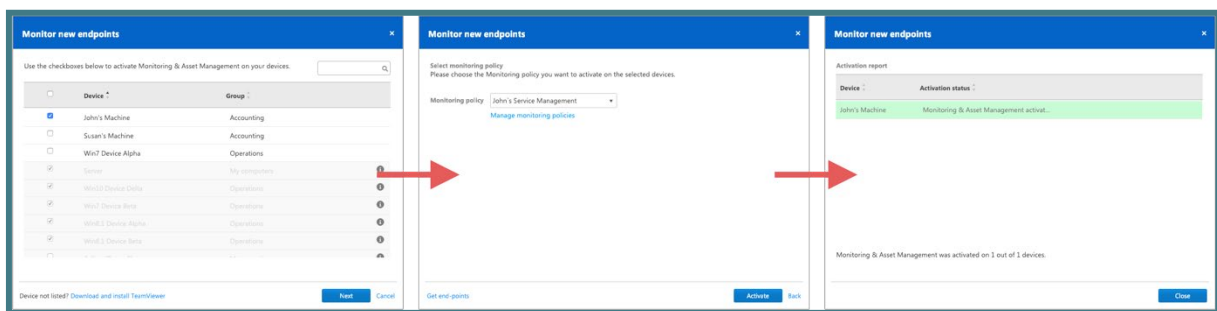


Image: Bulk activation via TeamViewer MCO 3.

3.2. Policies

Policies are defined as individual settings which are sent to the endpoints once applied.

They contain all necessary information on how the service will:

- Remotely manage the device.
- Alert the user if something is not working properly.
- Setup thresholds and parameters.
- Send e-mail notifications.

Monitoring policies: determine the criteria your devices will be set to for reporting when something is not running within the assigned thresholds or parameters.

Asset Management policies: determine the criteria based on which missing patches will be automatically deployed.

Endpoint Protection policies: determine when and to what extent your devices are scanned and protected against malware.

Backup policies: determine when and to what extent the files on your devices will be backed up.

3.2.1. Default Policy and Policy Options

For each service, a default policy is created when the first endpoint is activated.

1. The default policies will be applied to each activated endpoint if no other policy is specified when activating the endpoint.
2. The default policies can be changed at any time.
3. Newly created policies can be assigned as default policies.

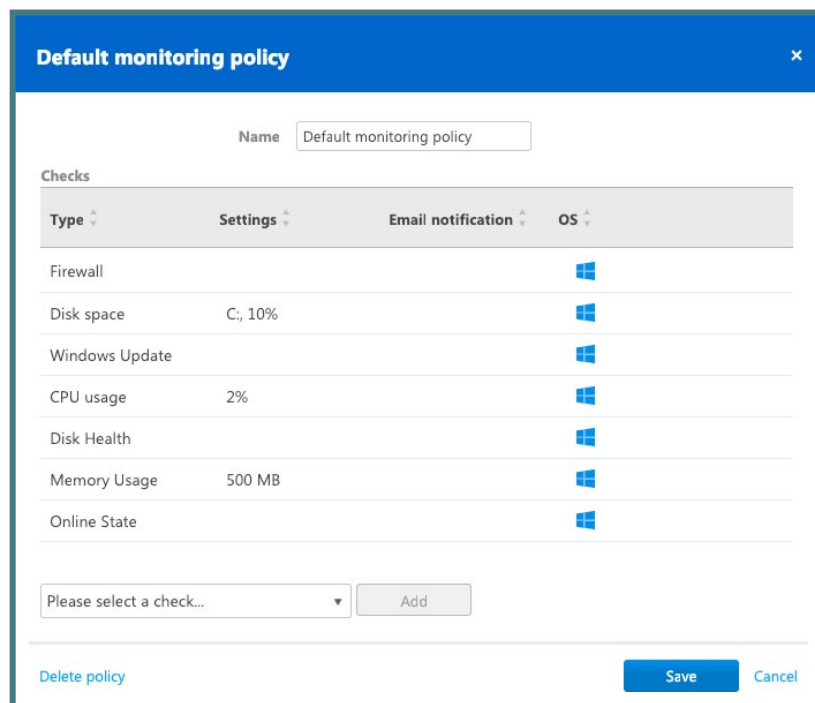


Image: Monitoring default policy.

Find all policies under:

Remote Management → Service name tab → Tools icon → Policies

In the Policies window you can:

1. Create a Policy.
2. Edit a policy.
3. Duplicate a policy.

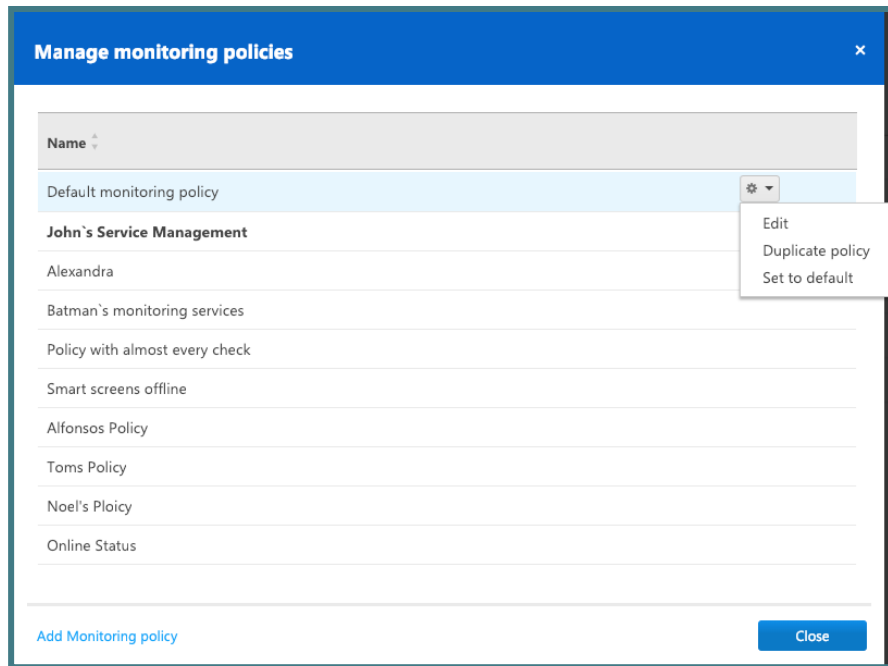


Image: Manage Monitoring policies.

3.2.2. Assign a Policy

Single policy assignment

You can assign a policy to each device by going to the desired service Tab and selecting the policy column on the right side of the Device view. Click the check mark to save.

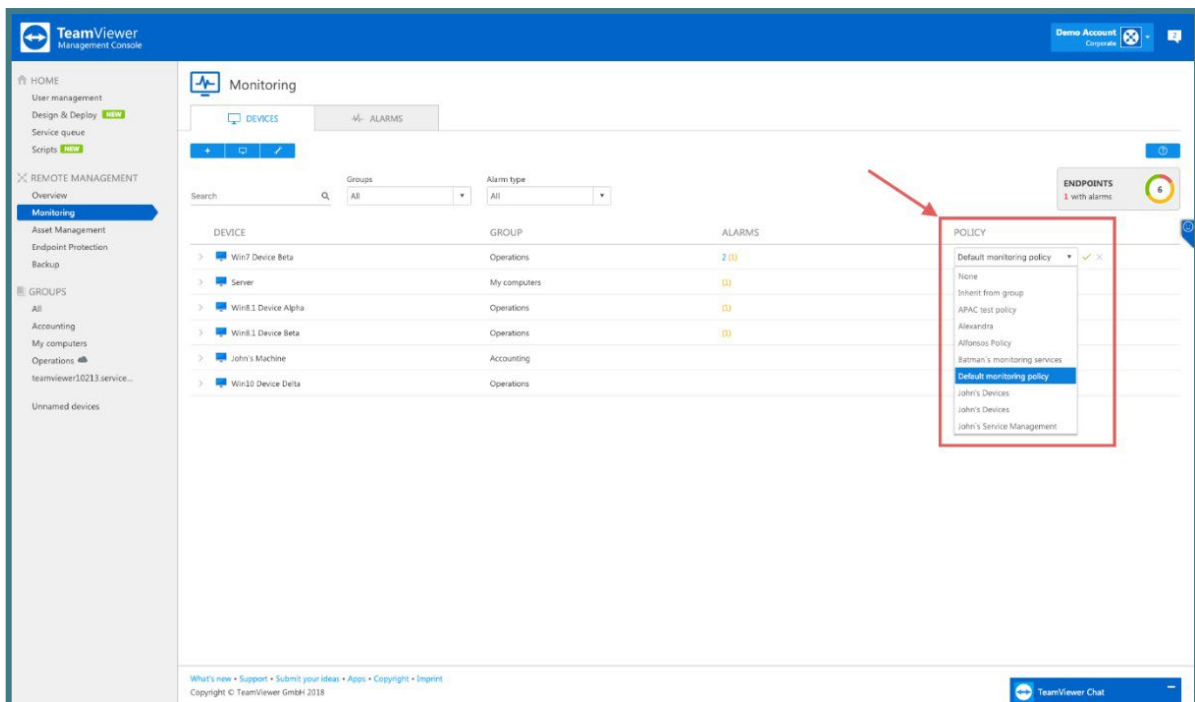


Image: Single policy assignment.

Group policy assignment

If you would like to have a policy for an entire group of computers, select 'Inherit from group' located in the Policy row for all computers in a group (you can also filter by individual groups). Click the check mark to save.

4. Go to the left pane of the desired group.
5. Hover over the group.
6. Click on the pen icon, and then click 'edit.'
7. Select the policy for the desired service and click save.

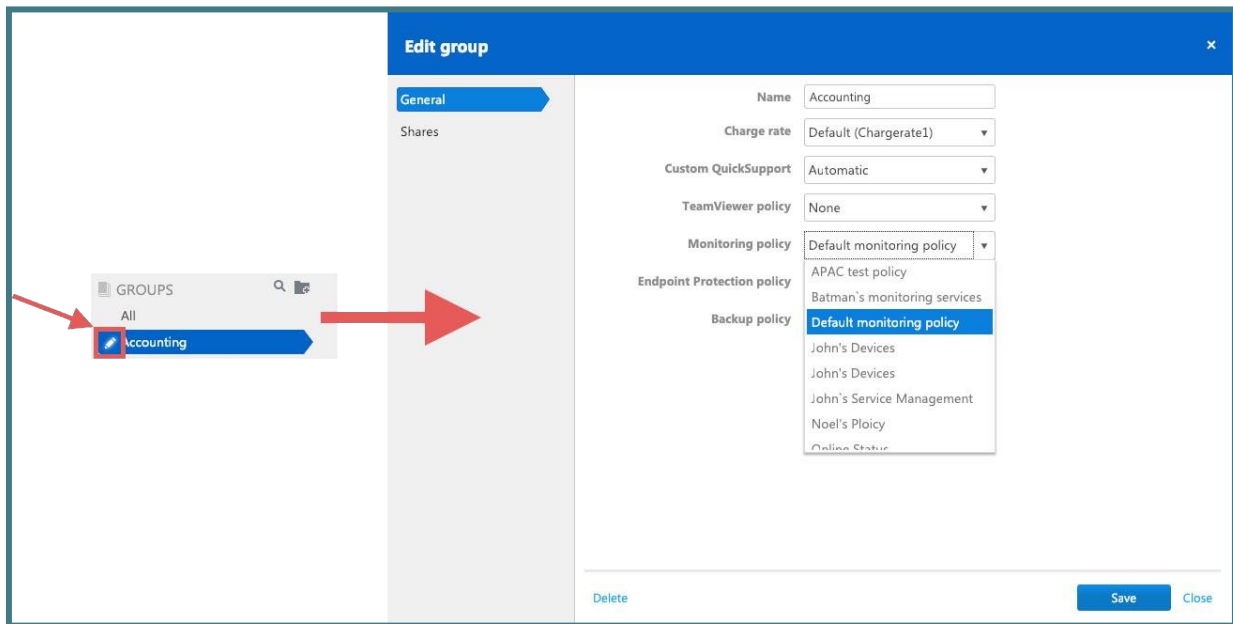


Image: Group policy assignment.

4. Monitoring & Asset Management

To monitor your devices and manage your IT assets, use the service **TeamViewer Monitoring & Asset Management**.

Monitoring policies will define the proactive behaviors of individual checks assigned to devices.

For **license activation**, please see [2.2 License Activation](#).

For **system requirements**, please see [2.3 System Requirements](#).

For **configuring policies** and assigning them to a device, please see [3.2 Policies](#).

When all defined conditions for a check are met, an alert is triggered and displayed as an alarm message in the TeamViewer Management Console and in the TeamViewer full version. An e-mail notification will also be sent if configured in the policy. An alert message indicates that a problem has occurred on one of the monitored devices.

4.1. Monitoring & Asset Management Activation

For activation of endpoints please see: [3.1 Activation](#).

4.2. Monitoring Checks

Monitoring checks are categorized in 3 Categories which will help you determine how critical the situation is on a device.

Windows Checks



Image: The three categories of monitoring checks.

1. Health and Security

- a. Online state
 - i. This is a proactive check which will alert the user when the device goes offline and comes back online.
 - ii. When the check is applied to a device, it will monitor if the system has internet connectivity. When the device goes offline for more than 1 minute an alert will be triggered.
 - iii. After the device goes offline it will track of length of time in this state. Additionally, when the device comes back online a recovery notification will be generated and the state of the check will return to green.
 - iv. The check can be customized with a time delay of 5 or 10 minutes. When selecting a time delay, the online state will be reported only after the device is offline for more than the time delay value selected.
- b. Windows Update
 - i. This check will alert the user if the Windows Update is turned off.
 - ii. Users will see if there are available updates that can be installed on the device.
 - iii. A variation of both 'Windows Update is off' or 'Updates are available' can be selected. An alert will be triggered if one of the variables is met.
- c. Antivirus
 - i. This check will be triggered if the installed security solution, which is registered in Windows Security, is off or if the malware definition updates failed to be updated for more than 2 days.

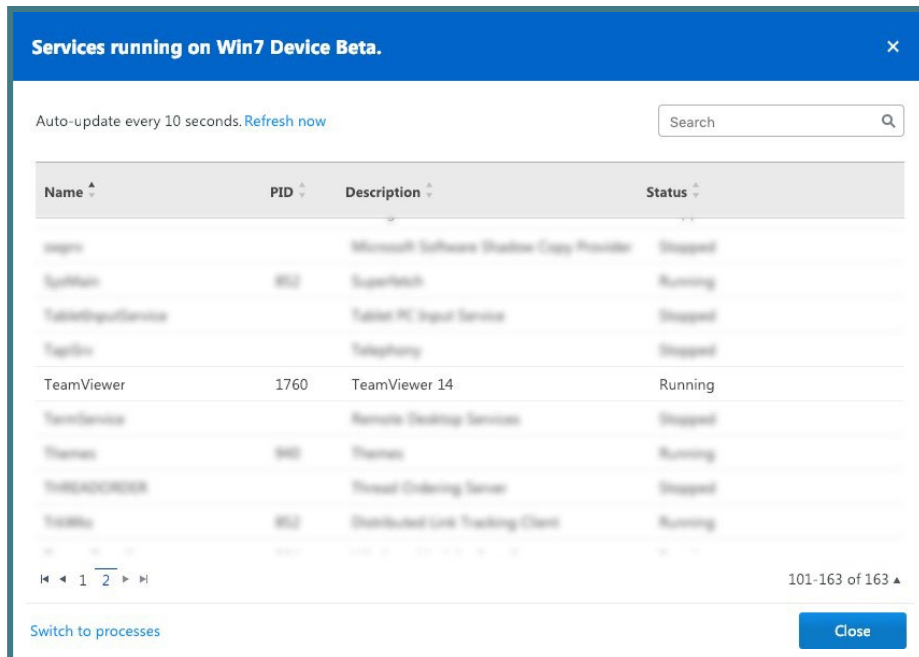


Image: Software operation check in the Management Console.

Note: Running services can be viewed by opening the Remote Task Manager.

b. Processes

- i. This check will monitor a defined Windows process, and it will trigger an alert if the process is running or not running.
- ii. In order to set up this check, the exact process name must be added in the check configuration menu.
- iii. The name of the process is case sensitive.

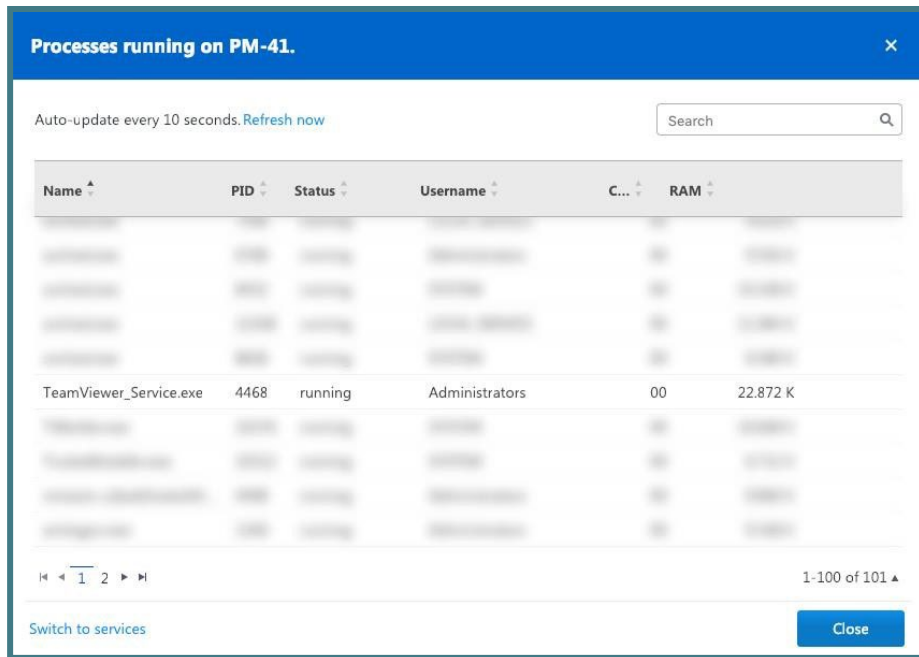


Image: Process check in the Management Console.

Note: Running processes on a device can be viewed by opening the Remote Task Manager.

c. Event Log

- i. This check will report event logs from the Windows Event Viewer after an entry is written in the configured logs folder.
- ii. Many applications and critical windows operations record logs making the event log checks a very powerful check to monitor key operations on a Windows device.
- iii. In order to set up this check, the queried category needs to be selected:
 1. Security
 2. Application
 3. System
- iv. After selecting the folder where the logs will be monitored, the source needs to be selected.
- v. After selecting the source, the event ID needs to be added. Multiple event ID's can be added separated by “,” (comma).
- vi. After selecting the ID, one or more event log categories needs to be selected:
 1. Audit
 2. Information
- vii. When an event log is written and matches the predefined check settings, a notification is sent. A full description of the triggered event log will be outlined in the e-mail.

3. Hardware

- a. Disk Space
 - i. This check will monitor the free space on a system drive and will report when the free space is less than the defined value.
 - ii. Multiple disk space checks can be added to one policy with different drive letters.
 - iii. In order to set up the disk space check, first select the desired drive that needs to be monitored on the device, e.g. C:\ or G:\.
 - iv. After selecting the drive, select the needed variable:
 - 1. % - percentage of free space left on drive.
 - 2. GB –Gigabytes of free space left on drive.
 - 3. MB –Megabytes of free space left on drive.
 - v. After selecting the variable, enter the minimum threshold value. Whenever the disk space falls below this value, an alert will be triggered.
- b. Disk Health
 - i. This check will report any S.M.A.R.T. errors recorded in the Windows Management Instrumentation module.
 - ii. S.M.A.R.T. is a standardization of error reporting for storage device components. More details can be read here: <https://en.wikipedia.org/wiki/S.M.A.R.T.>
 - iii. When an error is triggered, it will be reported, and then an alert will be sent.
 - iv. If configured, an e-mail notification will also be sent containing all necessary error reports including the recorded error.
 - v. If S.M.A.R.T. alerts for a device continue to be triggered, please investigate the reported errors on the manufacturers' web resources, or use the dedicated tools created by the hardware manufacturer.
- c. Memory Usage
 - i. This check will monitor the amount of free Random-Access Memory or RAM on the device.
- d. CPU Usage
 - i. This check will monitor the CPU usage on the device and an alert will be triggered if the usage is higher than the defined percentage in the check configuration menu.

macOS Checks

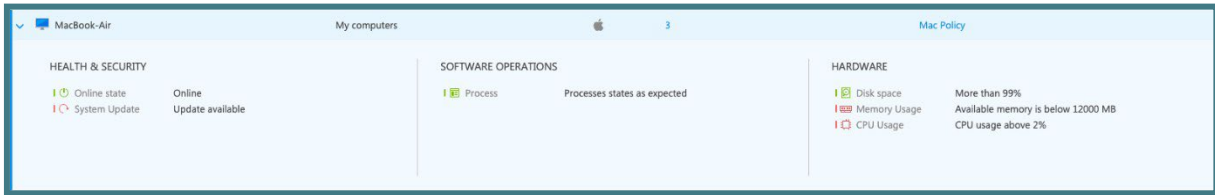


Image: The three categories of monitoring checks.

1. Health and Security

a. Online state

- i. This is a proactive check which will alert the user when the device goes offline and comes back online.
- ii. When the check is applied to a device, it will monitor if the system has internet connectivity. When the device goes offline for more than 1 minute an alert will be triggered.
- iii. After the device goes offline it will track of length of time in this state. Additionally, when the device comes back online a recovery notification will be generated and the state of the check will return to green.
- iv. The check can be customized with a time delay of 5 or 10 minutes. When selecting a time delay, the online state will be reported only after the device is offline for more than the time delay value selected.

b. System Update

- i. This check will alert the user if a System Update is available

2. Software Operations

a. Processes

- i. This check will monitor a defined process, and it will trigger an alert if the process is running or not running.
- ii. In order to set up this check, the process name listed in "Activity Monitor" must be added in the check configuration menu.

3. Hardware

e. Disk Space

- i. This check will monitor the free space on a system drive and will report when the free space is less than the defined value.
- ii. Multiple disk space checks can be added to one policy with different drive letters.
- iii. In order to set up the disk space check, first add the "volume path" that must be monitored (e.g. Macintosh HD)
- iv. After selecting the drive, select the needed variable:
 1. % - percentage of free space left on drive.
 2. GB –Gigabytes of free space left on drive.
 3. MB –Megabytes of free space left on drive.
- v. After selecting the variable, enter the minimum threshold value. Whenever the disk space falls below this value, an alert will be triggered.

f. Memory Usage

- i. This check will monitor the amount of free Random-Access Memory or RAM on the device.

- g. CPU Usage
 - i. This check will monitor the CPU usage on the device and an alert will be triggered if the usage is higher than the defined percentage in the check configuration menu.

Linux Checks

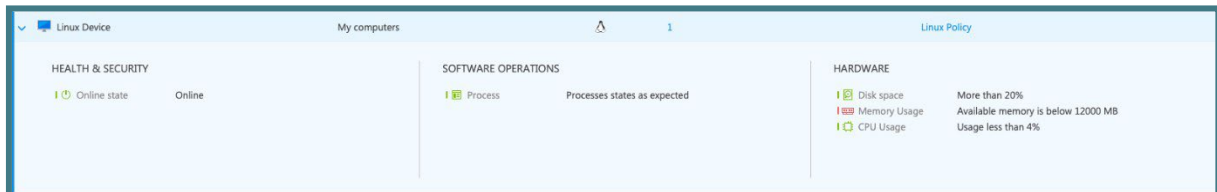


Image: The three categories of monitoring checks.

1. Health and Security

- a. Online state
 - i. This is a proactive check which will alert the user when the device goes offline and comes back online.
 - ii. When the check is applied to a device, it will monitor if the system has internet connectivity. When the device goes offline for more than 1 minute an alert will be triggered.
 - iii. After the device goes offline it will track of length of time in this state. Additionally, when the device comes back online a recovery notification will be generated and the state of the check will return to green.
 - iv. The check can be customized with a time delay of 5 or 10 minutes. When selecting a time delay, the online state will be reported only after the device is offline for more than the time delay value selected.
- b. System Update
 - i. This check will alert the user if a System Update is available

2. Software Operations

- a. Processes
 - i. This check will monitor a defined process, and it will trigger an alert if the process is running or not running.
 - ii. In order to set up this check, the process file name or the absolute path of a process (e.g. filename: bash or teamviewerd ; absolute path: /usr/bin/bash or /opt/teamviewer/tv_bin/teamviewerd) must be added in the check configuration menu.

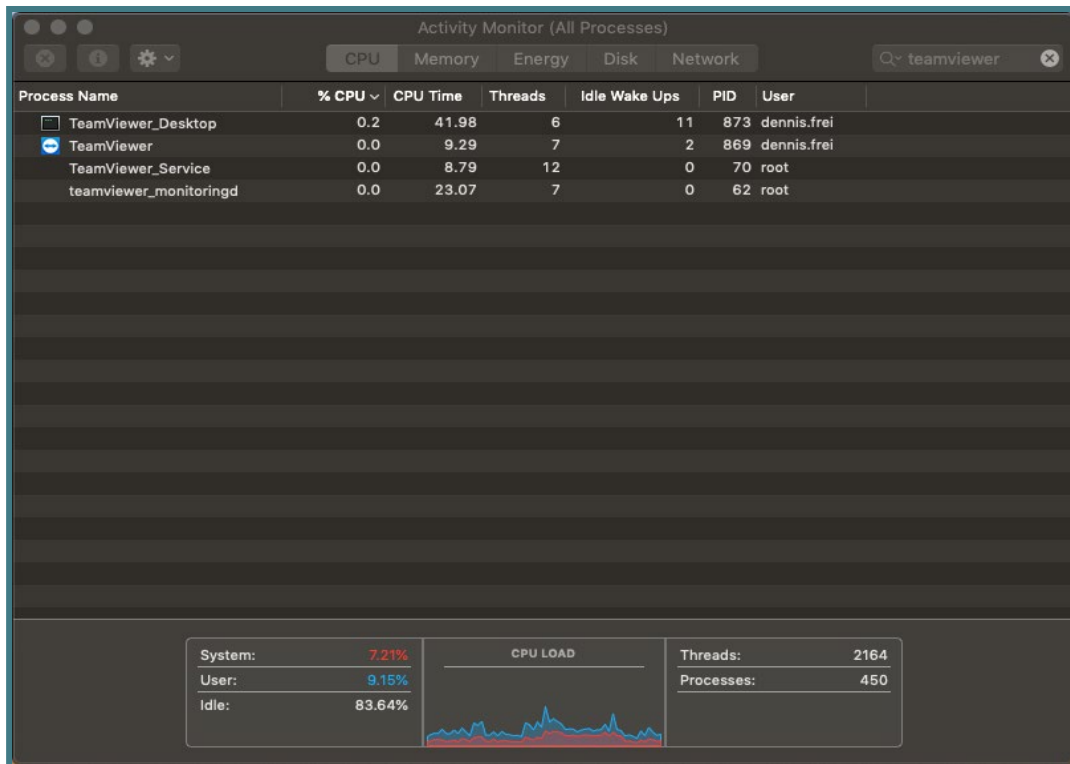


Image: Activity monitor and service.

3. Hardware

a. Disk Space

- i. This check will monitor the free space on a system drive and will report when the free space is less than the defined value.
- ii. Multiple disk space checks can be added to one policy with different drive letters.
- iii. In order to set up the disk space check, first add the “mount point” that must be monitored (e.g. /home or /media/data)
- iv. After selecting the drive, select the needed variable:
 1. % - percentage of free space left on drive.
 2. GB –Gigabytes of free space left on drive.
 3. MB –Megabytes of free space left on drive.
- v. After selecting the variable, enter the minimum threshold value. Whenever the disk space falls below this value, an alert will be triggered.

b. Memory Usage













- i. This check will monitor the amount of free Random-Access Memory or RAM on the device.

c. CPU Usage

- i. This check will monitor the CPU usage on the device and an alert will be triggered if the usage is higher than the defined percentage in the check configuration menu.

4.3. Monitoring Policy

The *default Monitoring & Asset Management policy* includes the following checks, described in 4.2 Monitoring Checks.

- Is antivirus software installed and active? 
- Is more than 500 MB of RAM available?   
- Is CPU usage higher than 75%?   
- What is the health of the hard drive? 
- Is the available disk space less than 10%? 
- Is Windows Update active?  
- Is the Windows Firewall activated? 

For more policy options please read: 3.2 Policies.

4.4. Remote Task Manager

The Remote Task Manager can be opened for every device that has Monitoring & Asset Management installed. (Windows)

The window will display a current list of processes or services on the remote device which can be terminated if necessary.

Note: This is a very important tool when users need to troubleshoot a remote computer *without* connecting to it remotely.

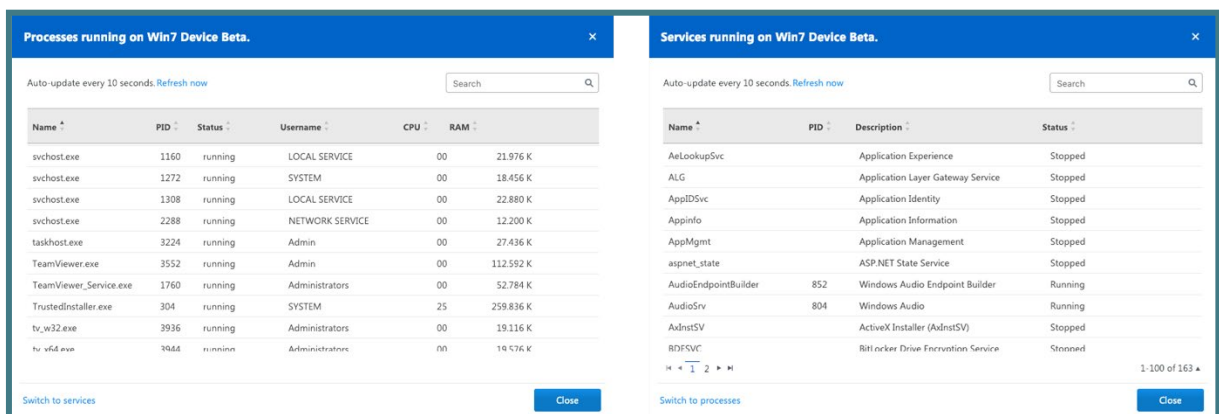


Image: Remote Task Manager.

4.5. Alarms and Notifications

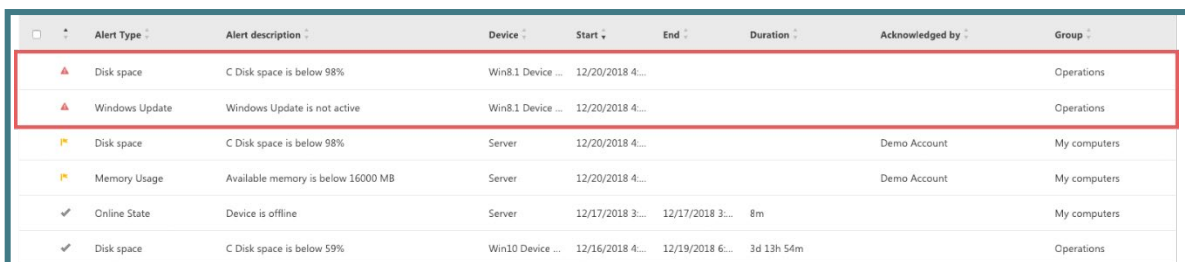
4.5.1. Alarms

Alarms are generated when there is a risk of breaching a set threshold defined in the monitoring policy.

Alarms are displayed in the TeamViewer Management Console and TeamViewer application.

There are several alarm types:

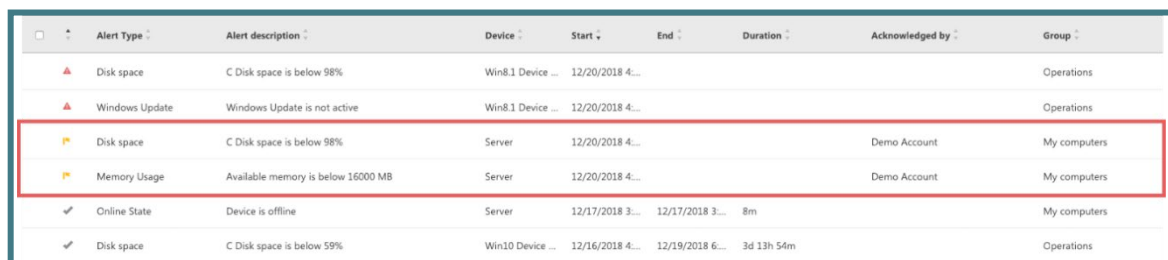
1. Raised Alarm
 - a. When a check is at risk for breaking its configured threshold, an alarm will be created and reported in the management console.
 - b. The alarm can be identified by a red triangle.



Alert Type	Alert description	Device	Start	End	Duration	Acknowledged by	Group
▲ Disk space	C Disk space is below 98%	Win8.1 Device ...	12/20/2018 4:...				Operations
▲ Windows Update	Windows Update is not active	Win8.1 Device ...	12/20/2018 4:...				Operations
⚠ Disk space	C Disk space is below 98%	Server	12/20/2018 4:...			Demo Account	My computers
⚠ Memory Usage	Available memory is below 16000 MB	Server	12/20/2018 4:...			Demo Account	My computers
✓ Online State	Device is offline	Server	12/17/2018 3:...	12/17/2018 3:...	8m		My computers
✓ Disk space	C Disk space is below 59%	Win10 Device ...	12/16/2018 4:...	12/19/2018 6:...	3d 13h 54m		Operations

Image: Raised alarm.

2. Acknowledged Alarm
 - a. A raised alarm can be acknowledged by the user. Once this is done, the alarm will become 'Acknowledged.'
 - b. Acknowledging the alarm does not mean that the problem is resolved. It only means that the supporter acknowledged that there is a problem, and will fix it later because issue is not critical enough to be fixed immediately.



Alert Type	Alert description	Device	Start	End	Duration	Acknowledged by	Group
▲ Disk space	C Disk space is below 98%	Win8.1 Device ...	12/20/2018 4:...				Operations
▲ Windows Update	Windows Update is not active	Win8.1 Device ...	12/20/2018 4:...				Operations
⚠ Disk space	C Disk space is below 98%	Server	12/20/2018 4:...			Demo Account	My computers
⚠ Memory Usage	Available memory is below 16000 MB	Server	12/20/2018 4:...			Demo Account	My computers
✓ Online State	Device is offline	Server	12/17/2018 3:...	12/17/2018 3:...	8m		My computers
✓ Disk space	C Disk space is below 59%	Win10 Device ...	12/16/2018 4:...	12/19/2018 6:...	3d 13h 54m		Operations

Image: Acknowledged alarm.

3. Recovered/Cleared Alarm

- a. When a raised alarm returns to the defined threshold, the alarm will recover automatically.
- b. The majority of monitoring checks will attempt every minute to analyze if the thresholds are breached or recovered. If the checks have a configured time delay, they will check based on the time delay (e.g. online state check with a 10-minute delay configured).

Alert Type	Alert description	Device	Start	End	Duration	Acknowledged by	Group
▲ Disk space	C Disk space is below 98%	Win8.1 Device ...	12/20/2018 4:...				Operations
▲ Windows Update	Windows Update is not active	Win8.1 Device ...	12/20/2018 4:...				Operations
▣ Disk space	C Disk space is below 98%	Server	12/20/2018 4:...			Demo Account	My computers
▣ Memory Usage	Available memory is below 16000 MB	Server	12/20/2018 4:...			Demo Account	My computers
✓ Online State	Device is offline	Server	12/17/2018 3:...	12/17/2018 3:...	8m		My computers
✓ Disk space	C Disk space is below 59%	Win10 Device ...	12/16/2018 4:...	12/19/2018 6:...	3d 13h 54m		Operations

Image: Recovered alarm.

4.5.2. Notifications

E-mail Notifications can be set up in the Monitoring policy. E-mail addresses accepted by the system are the ones which are recognized by the TeamViewer account or company profile:

- For TeamViewer accounts, the e-mail address needs to be in the contact list as a contact.
- For TeamViewer company profiles, the e-mail address needs to be a contact or a user in the company profile.

E-mail notifications are sent from: notification@teamviewer-rm.com

Note: if working with proxy or custom firewalls, a whitelist to the domain *.teamviewer-rm.com can be added.

E-mail notifications regarding raised or recovered alarms will contain the following information:

- Name of the Device where the alert was raised
- TeamViewer ID
- Date and time when the alarm was raised.
- Name of the check and the predefined threshold.
- Alarm description:
 - Check specific information will be written.
 - This will be different for each check.
- Possible actions:
 - Acknowledge alarm link
 - View Monitoring Report link.

- Connect to device link.

4.6. Monitoring Device View

The device view is designed to display metrics relevant to each device that has Monitoring & Asset Management installed.

In the device view for Monitoring, the user can see all relevant checks that are within their thresholds and all checks that failed.

Every failed check can be acknowledged and rechecked individually if the user decides that the raised alarm is not critical for the operation of that device.

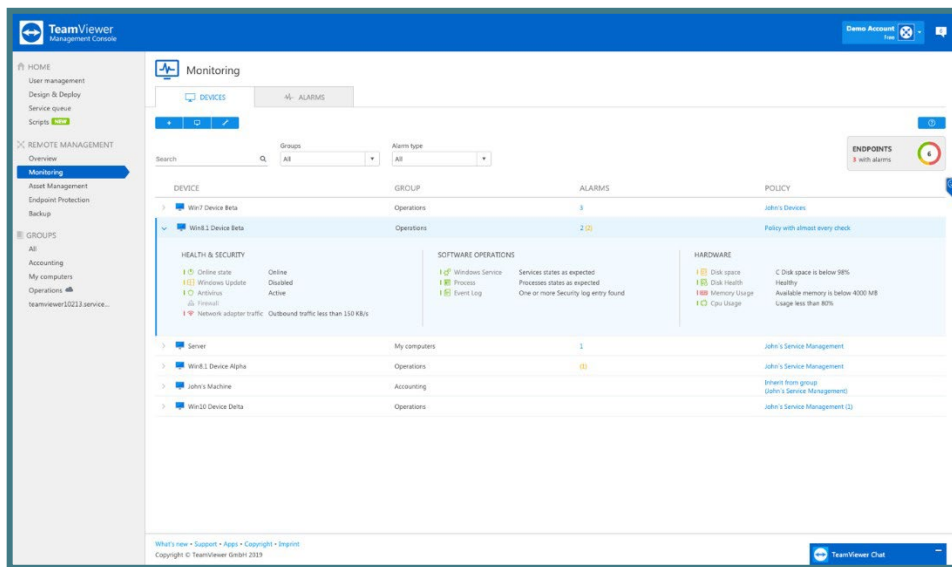


Image: Device view for Monitoring for Windows

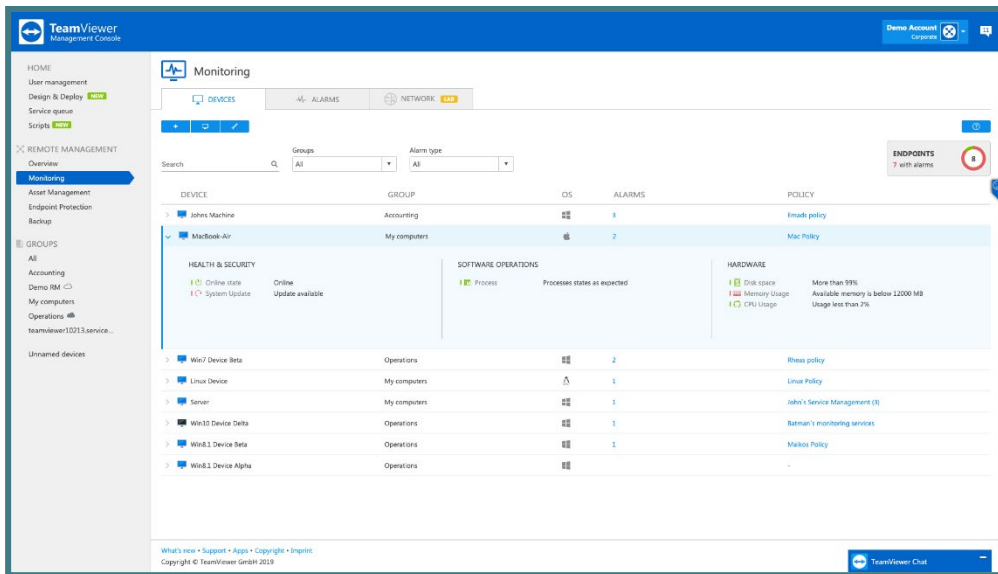


Image: Device view for Monitoring for macOS.

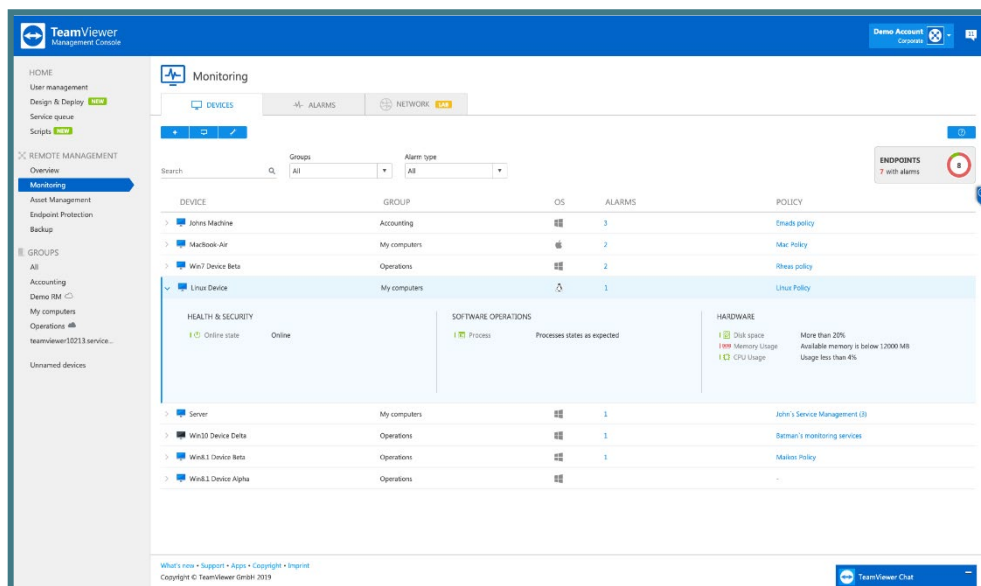


Image: Device view for Monitoring for Linux.

4.7. Monitoring Alarms View

The alarms view is focused on incident response. All raised alarms where the check threshold has been breached, organized, and exported.

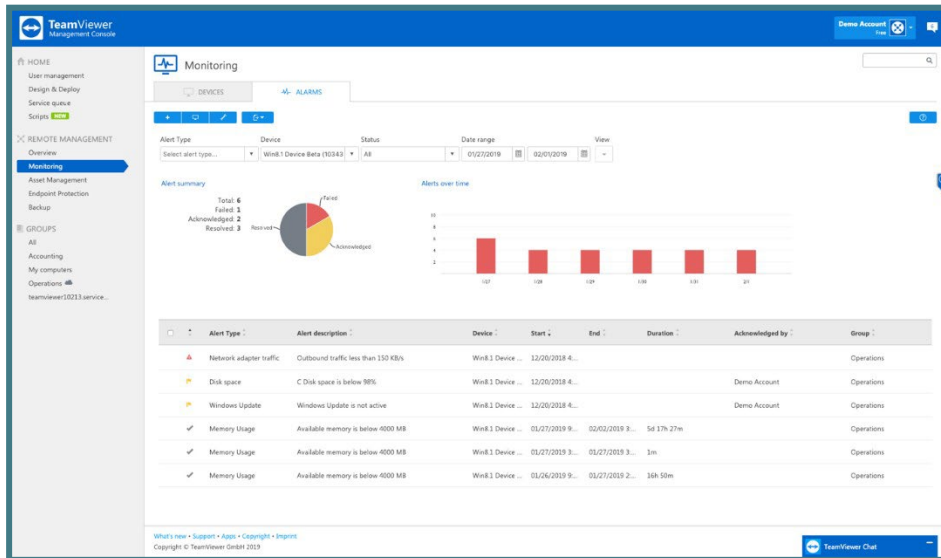


Image: Alarms view for Monitoring.

4.7.1. Monitoring Filtering

Filtering alarms will enable the user to get a comprehensive view based on need:

1. Filter by Alarm Type
2. Filter by Device
3. Filter by Alarm Status
4. Filter by Date Range

View settings can be used to check or uncheck the view structure of the reports:

1. Columns
 - a. Alert Type
 - b. Alert Description
 - c. Device
 - d. Start
 - e. End
 - f. Duration
 - g. Acknowledged by
 - h. Group
2. Group By
 - a. Alert Type
 - b. Device
 - c. Group by none
3. Other
 - a. Charts

4.7.2. Monitoring Export

After filtering monitoring alarms data, the export function can be used to export the Monitoring Alarms reports.

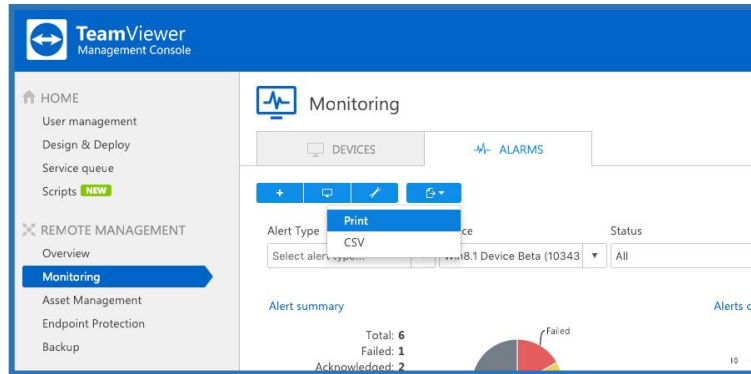


Image: Export feature in Monitoring.

Export to Print

This function will generate a web view that can be printed out or saved in any document format by using print plugins.

Export to CSV

This function will generate and download a CSV file that can be stored, managed, or modified as needed for auditability or other purposes.

4.8. Network Monitoring

To discover and monitor network devices within your local network use network monitoring by TeamViewer Monitoring.

With network monitoring, your discovered network devices will be sorted into one of the following categories:

- Computer – For all windows computers detected during the discovery process
- Router & Switch – For all routers and switches detected during discovery process
- Printer – For all network printers which were detected during discovery process
- UPS – For all universal power suppliers detected during discovery process
- NAS – For all network attached storages detected during discovery process
- Other Device – For all other devices which have an IP address and are available in your local network but do not fit into any other category

Network monitoring was released as a Laboratory version, so right now this feature can be used for free. In order to use network monitoring, you must have at least one license for TeamViewer

Monitoring, or you can test it during your trial period. When the TeamViewer Monitoring trial expires, network monitoring will also be deactivated in your account.

For TeamViewer Monitoring **license activation**, please see [2.2 License Activation](#).

For **system requirements**, please see [2.3 System Requirements](#).

4.8.1. Network Monitoring Activation

In order to activate network monitoring, TeamViewer Monitoring must be activated on the node* that will be discovering and monitoring your network devices. If you select a node that does not have TeamViewer Monitoring activated, the system will automatically install it on the node.

*Node: Is the device from which network monitoring will trigger a discovery, and will monitor your network devices. Each Node can discover its own local network.

Network monitoring can be activated in just a few clicks from the 'Network' tab in Remote Management → Monitoring:

1. Click on "Choose device" in the "Network" tab.
2. Select the appropriate device from your device list. The device should be online. Currently only Windows devices are supported.
3. Select the needed settings and click the 'DISCOVER' button.
 - a. Full Discovery
 - b. Custom discovery
 - i. Enter the IP range
 - ii. Enter the SNMP community string

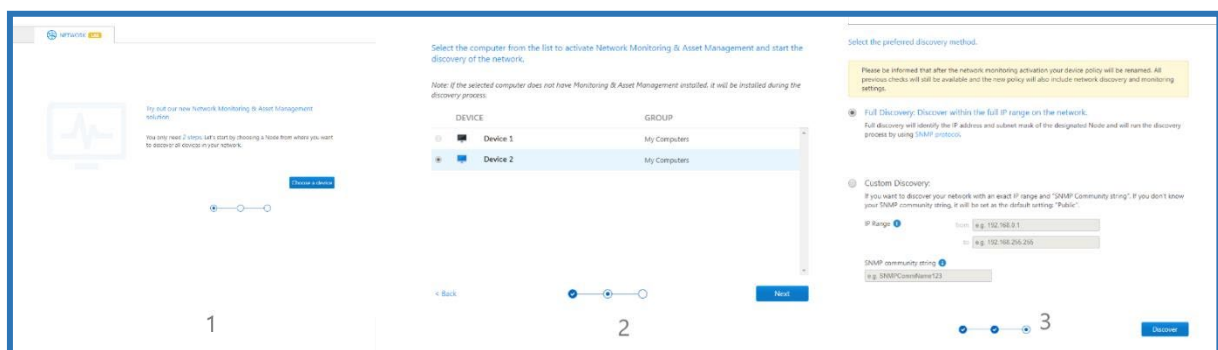
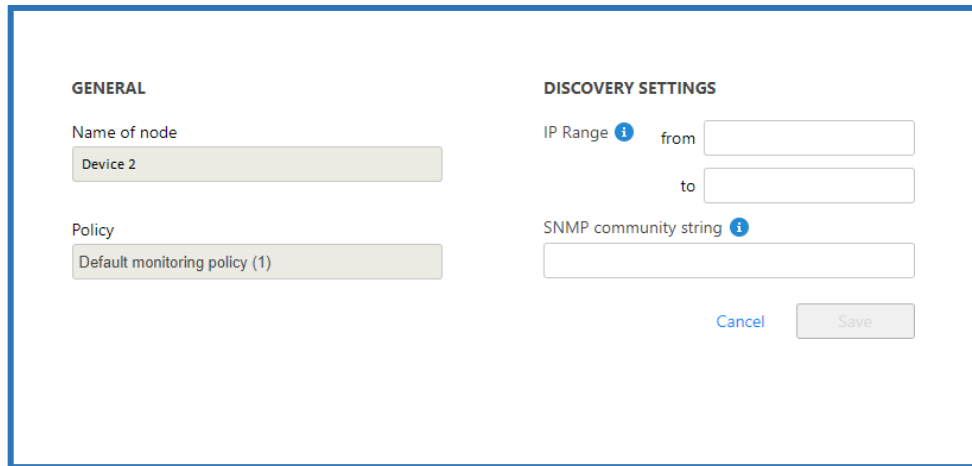


Image: Network monitoring activation.

After changing and saving the discovery settings, the system will start a discovery with the new settings in place. If you do not want to run a new discovery, press cancel.

4.8.2. Network Monitoring Settings

After the discovery is complete, you can always change the discovery settings from the settings menu.



The screenshot shows a settings page for network monitoring. It has two columns. The left column is titled 'GENERAL' and contains two text input fields: 'Name of node' with the value 'Device 2' and 'Policy' with the value 'Default monitoring policy (1)'. The right column is titled 'DISCOVERY SETTINGS' and contains an 'IP Range' section with 'from' and 'to' sub-inputs, and an 'SNMP community string' input field. At the bottom right of the right column are 'Cancel' and 'Save' buttons.

Image: Network monitoring settings page.

After changing and saving the discovery settings, the system will start a discovery with the new settings in place. If you do not want to run a new discovery, press cancel.

4.8.3. Network Monitoring Checks

After the discovery of network devices is complete, you can set up checks for periodical monitoring of your network devices. Currently, network monitoring supports the following checks:

For the **Router & Switch** category:

Port state: If selected, this will raise an alarm when a port from a router or switch is blocked or broken. This only works for devices with SNMP support.

For the **Network Attached Storage (NAS)** category:

Disk Space: If selected, this will raise an alarm when the NAS disk space is lower than the configured threshold. This only works for devices with SNMP support.

Disk Health: If selected, this will raise an alarm when the NAS disk health reports hardware errors. This only works for devices with SNMP support.

For the **Printer** category:

Toner: If selected, this will raise an alarm when the toner from a network printer is low. This only works for devices with SNMP support.

Paper: If selected, this will raise an alarm when the paper from a network printer is low. This only works for devices with SNMP support.

For the **Uninterruptible Power Supply (UPS)** category:

Battery capacity: If selected, this will raise an alarm when the UPS battery capacity falls below the configured threshold. This only works for devices with SNMP support.

Battery time remaining: If selected, this will raise an alarm when the UPS energy storage "in minutes" falls below the configured threshold. This only works for devices with SNMP support.

For the **Computer** category:

Monitor your computers with the TeamViewer Monitoring service.

Checks will run every 1 min. If any issue is detected, an alert will be displayed in the management console.

In addition to the above checks, users can see the IP address and on- and offline status for each discovered device.

Tip: network monitoring uses SNMP protocol for discovering and monitoring the network. In order to effectively monitor your network devices, SNMP should not be restricted in your local network.

4.8.4. Network Monitoring Policy

Please be informed that after activating network monitoring, your device policy will be renamed. All previous checks (TeamViewer Monitoring checks) will still be available, and the new policy will also include network discovery and monitoring settings.

You can open the policy page for network discovery from here:

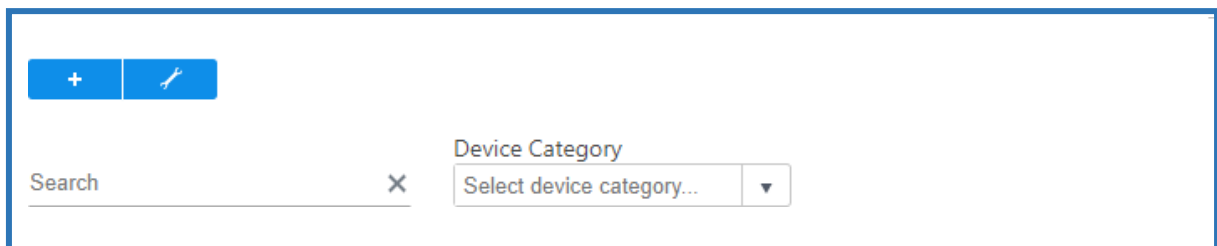


Image: Icon for opening network discovery policy

Next, choose which policy you want to edit, and select the needed checks for monitoring your network devices.

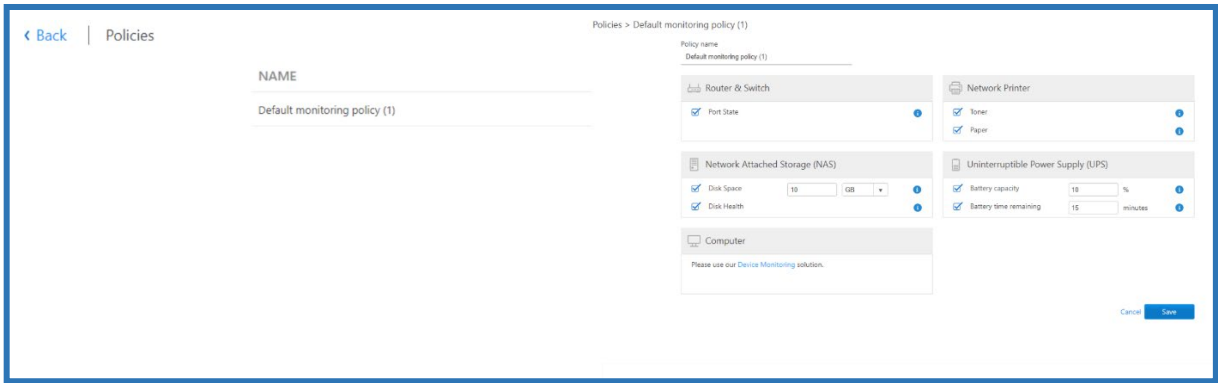


Image: Policy page for network discovery

4.8.5. Network Monitoring Views

There are 3 types of views for network monitoring:

All Node View: In this view you can see all your networks in one place with details about device quantity and alerts. Click on the Home button to get to this view.

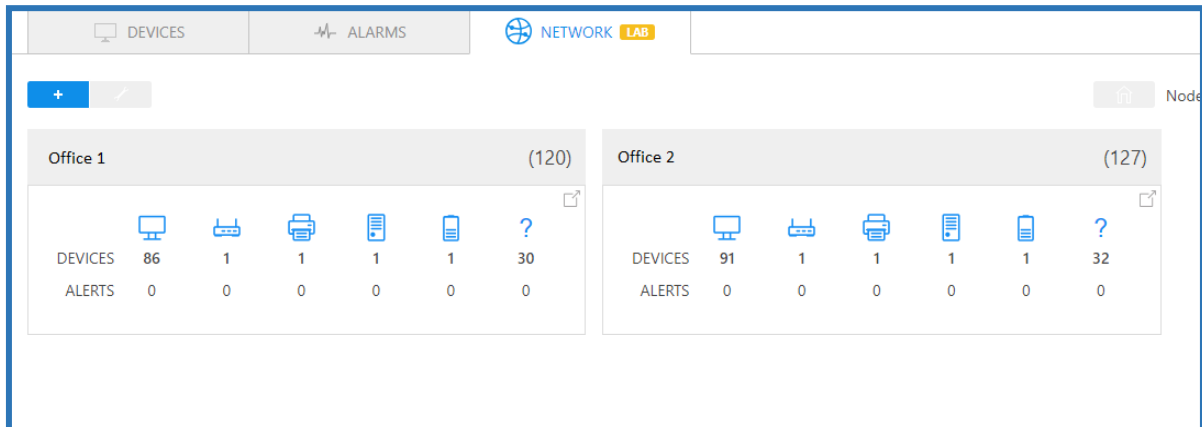


Image: All node view in network monitoring.

List View: In this view you can see all your networks in one place with details about device quantity and alerts. You can click on the Node header and go to list view for more details. You can also extend rows to see more details about each device.

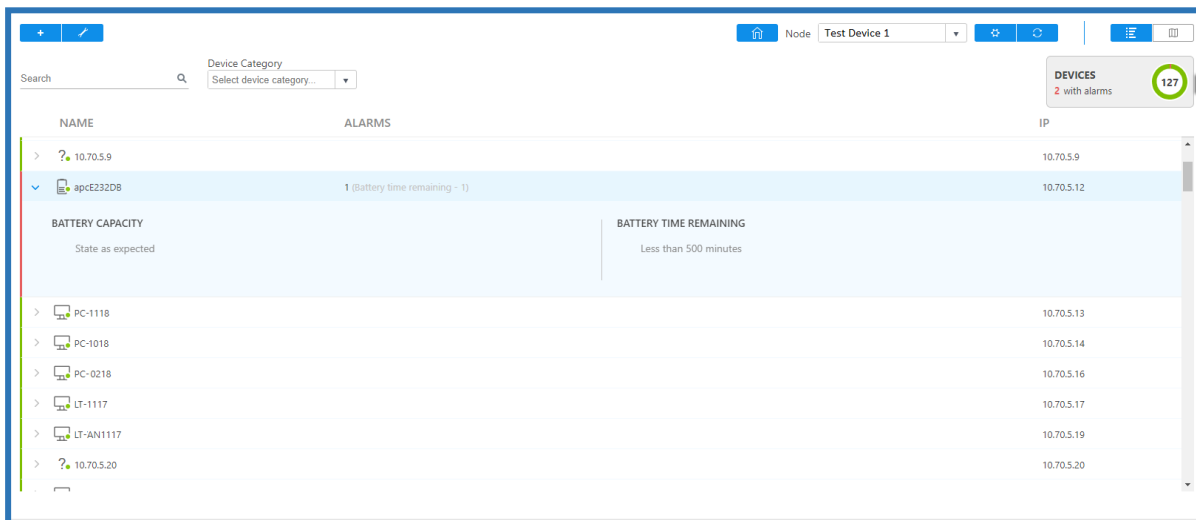


Image: List view of network monitoring.

Map view: Map view is under construction now. It will allow you to see the interconnections between discovered network devices.

4.9. Remote Scripting

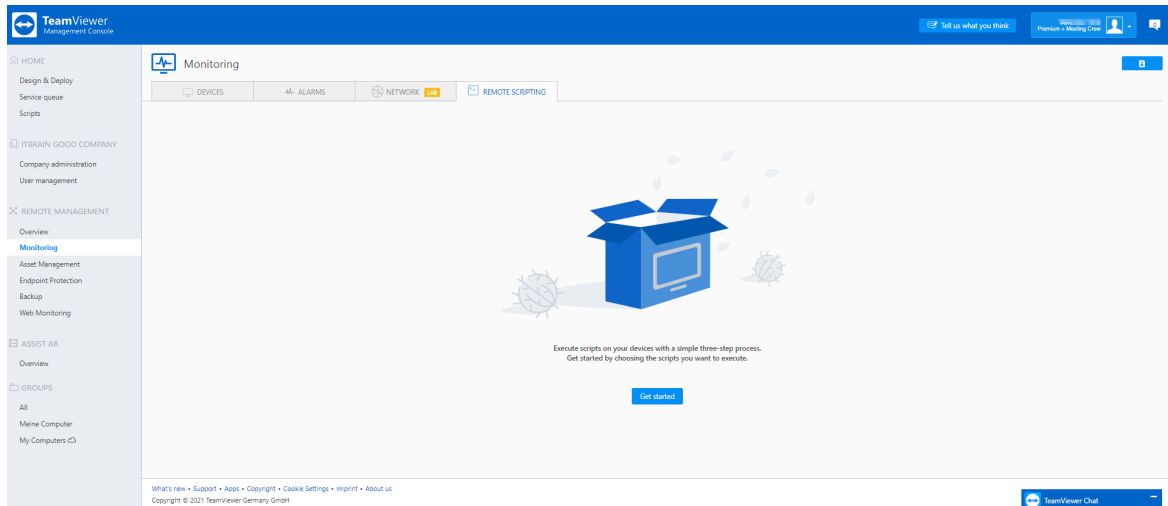
The Monitoring service now includes one-to-many Remote Scripting. This new feature allows you to execute scripts on your devices without establishing a TeamViewer session. Remote scripting provides you with the possibility to execute scripts on multiple devices at once and at the same time track your executions within the Script History log which contains a list of past and current executions.

The current version of Remote scripting supports only Microsoft Windows devices. The script format supported is batch(.bat), CMD(.cmd) and Powershell(.ps1).

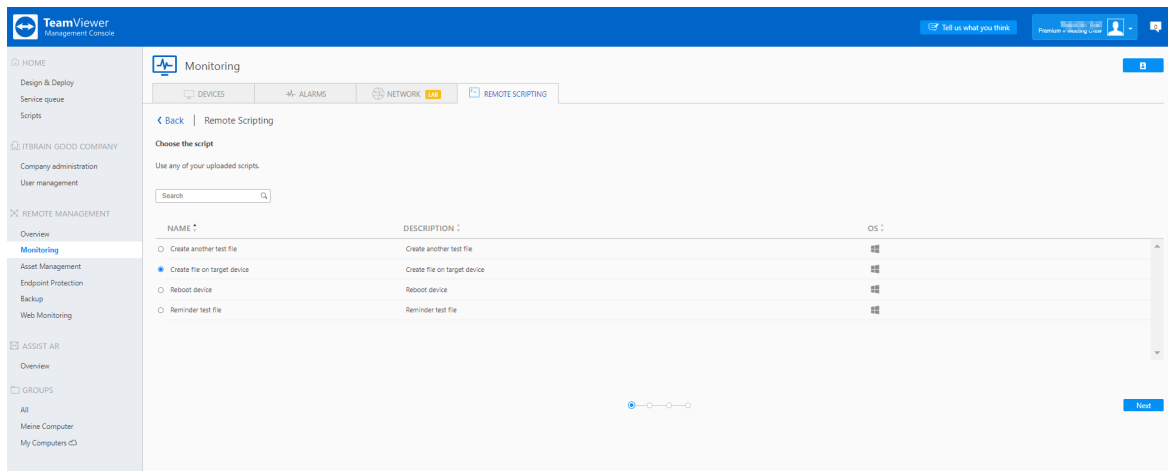
Script Execution flow:

In the Monitoring navigation menu, you will find a new tab called Remote Scripting. When you are using the feature for the first time you will see the view below. To execute a script, follow these steps:

Step 1: Click on Get started

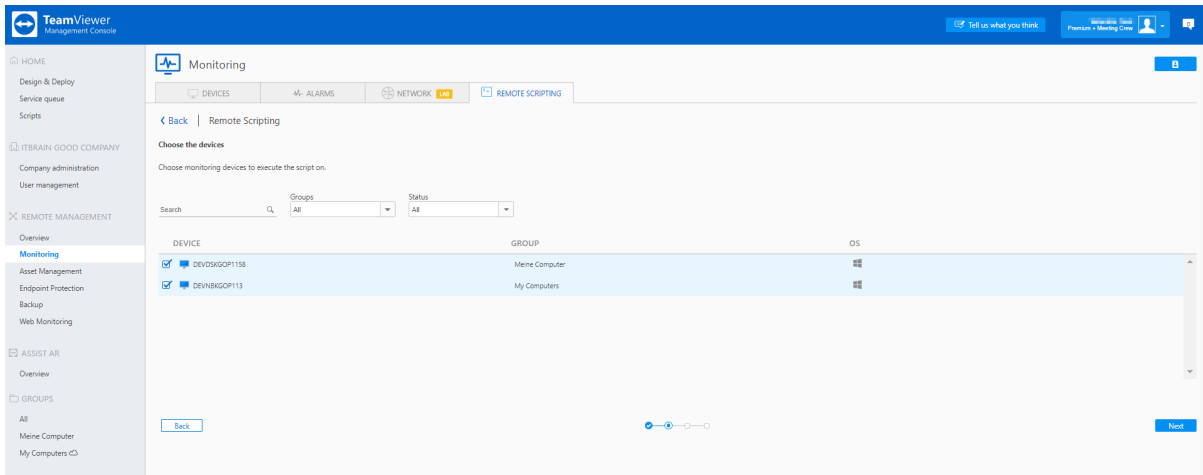


Step 2: Select the script you want to execute



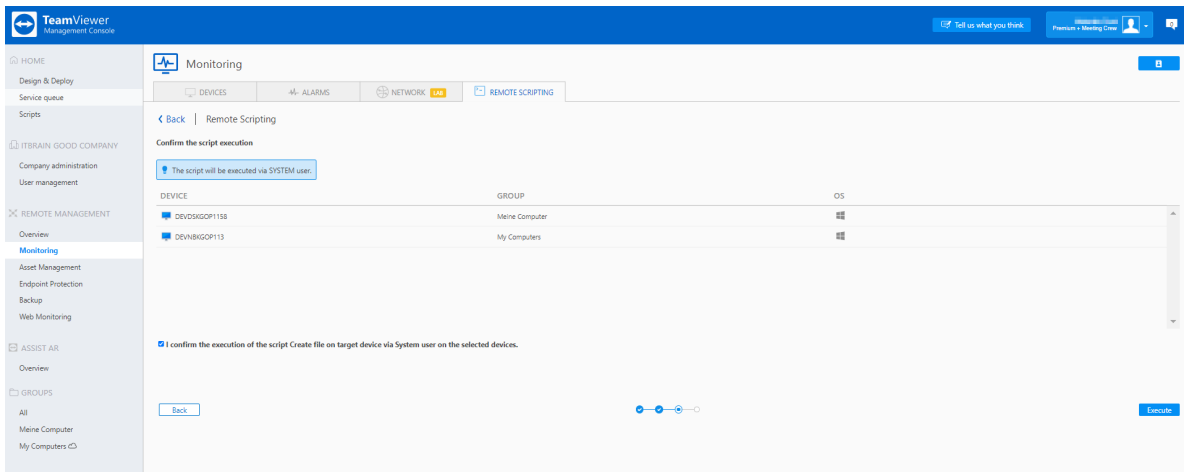
Once the script is selected, click on Next.

Step 3: Select the devices which you want to execute the script on



Once you have selected the devices, click on Next.

Step 4: Acknowledge and start the execution

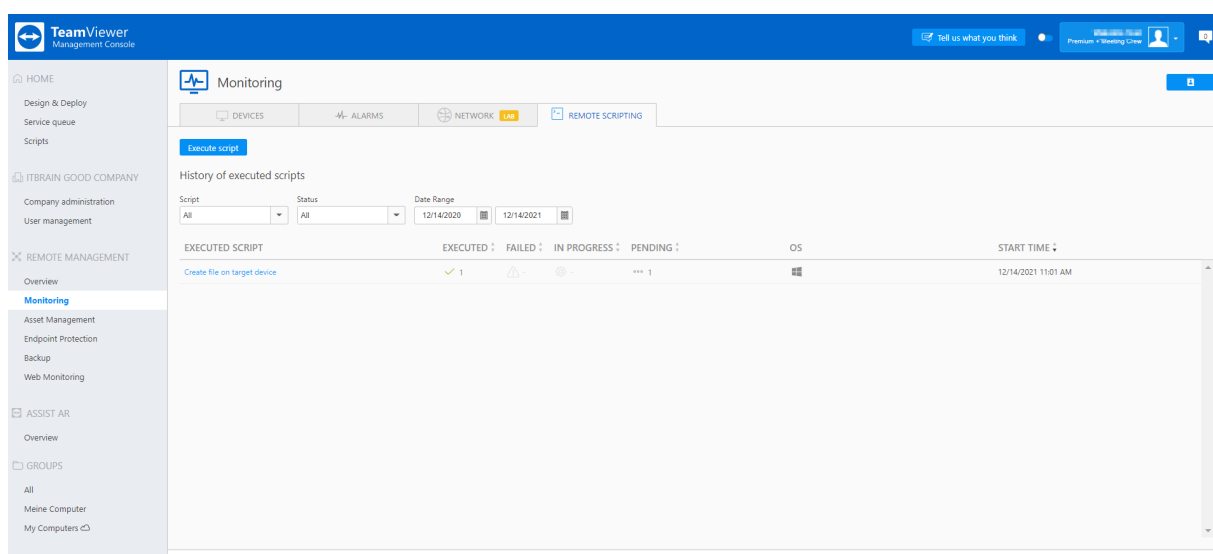


In this step you will see a summary of the execution details and in order to be able to execute you must confirm you want to proceed. Only when the confirmation box is ticked, the Execute button will be enabled.

After having confirmed, you can click on Execute. The script execution will now start.

History of executed scripts

The script history log is updated automatically when a script is being executed (see below)



There are 4 different states for each execution.

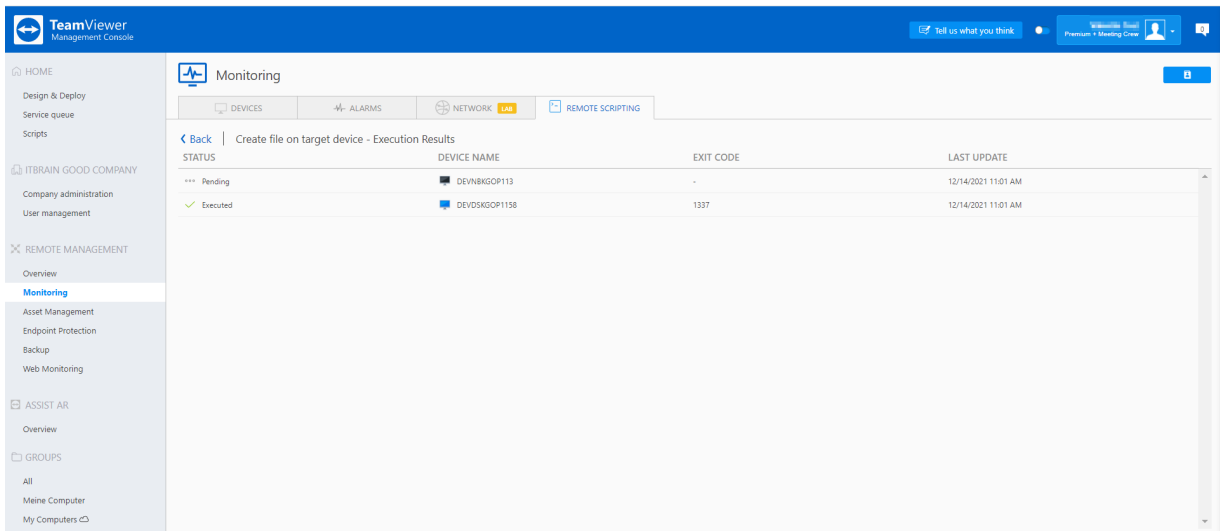
Executed – The script has been downloaded on the target device and execution has started

Failed – The script execution failed to initiate.

In Progress – The script is in progress.

Pending – The target device is offline and the script execution will start as soon as it comes back online.

For a detailed, device-specific view of the script execution, click on the script name in the history log view.



Our current version of Remote Scripting works with TeamViewer client version 15.22 or newer.

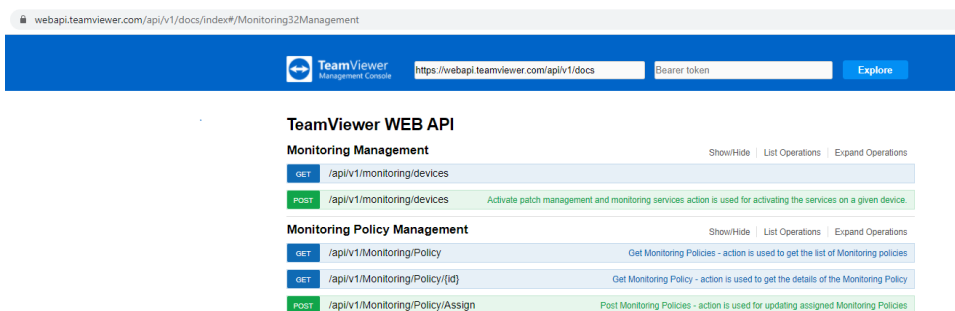
4.10. Monitoring API

Our web-based API allows you to access data and control various aspects of their TeamViewer account. You can use the API to develop apps that integrate TeamViewer functionality into own corporate environment or can develop apps that everyone can use.

The API uses REST to communicate with the application and the secure authorization standard OAuth 2.0 to manage access to data.

For more details see the [Develop Custom TeamViewer Solutions](#) web page and the API

Documentation - <https://webapi.teamviewer.com/api/v1/docs/index#/>



4.10.1. Monitoring API actions

- GET /api/v1/Monitoring/Policy - action is used to get the list of monitoring policies.
- GET /api/v1/Monitoring/Policy/{id} - action is used to get the details of the monitoring policy
- POST /api/v1/Monitoring/Policy/Assign - action is used for updating assigned monitoring policies

- POST /api/v1/Monitoring/devices - Activate action is used for activating patch management and monitoring services on a managed device.
- GET /api/v1/Monitoring - action is used to get the service activation information.

For more information – see the API [documentation](#)

4.11. Asset Management

After the installation of the Monitoring & Asset Management service, a snapshot of installed software and hardware will be collected and organized in the device view and asset view. Information about missing Patches will also be displayed in the Asset Management Device view. You will also be able to deploy software on the connected devices from the Software Deployment tab.

4.11.1. Device View

The screenshot displays the 'Asset Management' interface. On the left is a sidebar with navigation options: HOME, REMOTE MANAGEMENT, INTERNET OF THINGS, MANAGED GROUPS, and GROUPS. The main area shows a table of devices with the following columns: DEVICE, GROUP, OS, TEAMVIEWER, MISSING PATCHES, and POLICY. The table lists various devices such as 'DESKTOP-NAE7302', 'Chris Laptop', and 'DEMNKCLW926'. A 'Send Feedback' button is visible in the top right corner. A 'TeamViewer Chat' button is located at the bottom right of the interface.

DEVICE	GROUP	OS	TEAMVIEWER	MISSING PATCHES	POLICY
DESKTOP-NAE7302	Demo Group	Windows 10 Pro - 10.0.19041	v15.8.3	6	Inherit from group (verico)
Chris Laptop	My computers	Windows 10 Enterprise - 10.0.18363	v15.14.5	5	Aaron
DEMNKCLW926	My computers	Windows 10 Enterprise - 10.0.18362	v15.13937	-	-
DEMNKCLW977	My computers	Windows 10 Enterprise N - 10.0.17763	v15.7.6	13	Stella Policy
DEMNKGOPO38-Surface	My computers	Windows 10 Enterprise - 10.0.18362	v14.7.13736	15	-
NORAM TEAM DEMO -LT02	My computers	Windows 10 Enterprise - 10.0.18363	v15.14.5	9	test123
PC-demo0919	My computers	Ubuntu 18.04 (bionic) - GNU/Linux 5.0.0-23-gp...	v14.5.5819	-	-
Rob Laptop	My computers	Windows 10 Enterprise - 10.0.17134	v15.5.3	5	New Comp1
VM3	My computers	Windows 7 Professional - 6.1.7600	-	117	Stella Policy
Megami Desktop	New Folder	Windows 10 Enterprise - 10.0.18363	v15.8.3	10	Stella Policy
DEMNKCLW148	Sul	Windows 10 Enterprise - 10.0.19042	v15.14.5	5	Stella Policy
Training Laptop demo L13	Sul	Windows 10 Enterprise - 10.0.18363	v15.11.6	7	Inherit from group (National Raging)
Vanessa Demo	São Paulo	Windows 10 Enterprise N - 10.0.17763	v15.5.3	5	ABD Company
DEMNKCLW059	ZZZ	Windows 10 Enterprise - 10.0.18363	v15.15.5	7	ABD Company
DESKTOP-TSOVLMS	ZZZ	Undefined	-	5	Default Patch Management policy

Image: Device view in Asset Management.

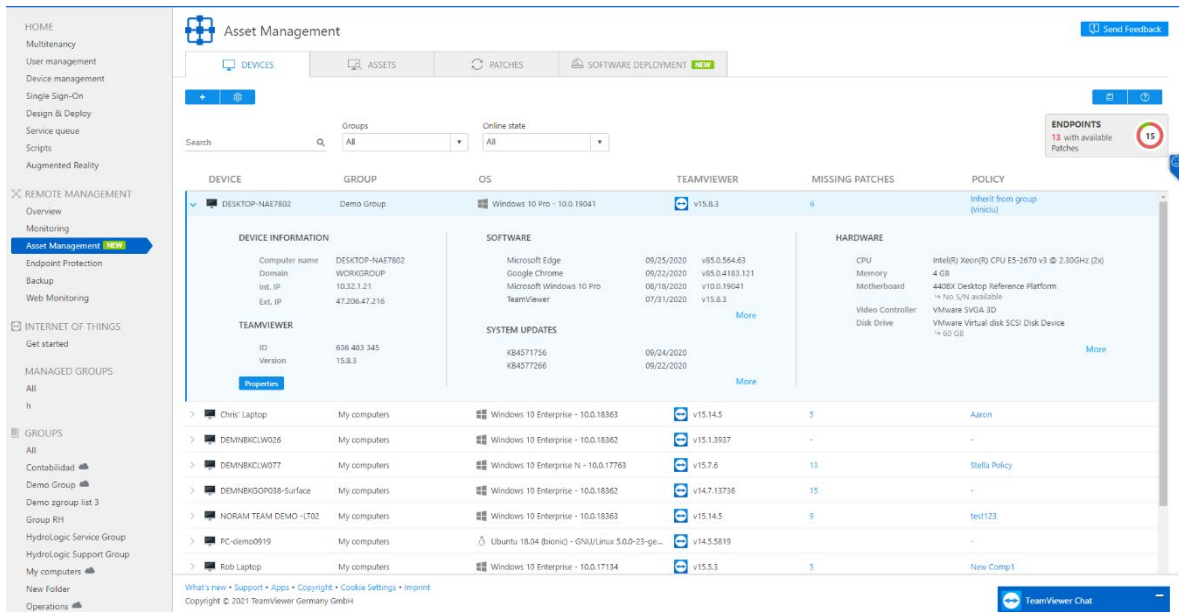


Image: Assets view within Asset Management for Windows.

The device view will sort and display the information in the following categories:

Device Information: Computer Name, Domain, Internal IP, External IP

Missing Patches count: OS and 3rd party missing patches count on selected machine.

TeamViewer: TeamViewer ID, TeamViewer version

Software: List of recently installed software (Windows, macOS)

Packages: List of all installed packaged in alphabetical order (Linux)

System Update: List of recently installed updates

Hardware: CPU name and model, physical memory (RAM), motherboard model and serial number (if available), video controller name and model, disk drives' name, model, capacity and serial number (if available).

4.11.2. Asset View

From the Asset view, reports can be generated based on the categories below and exported as a web view (print) or as a CSV file.

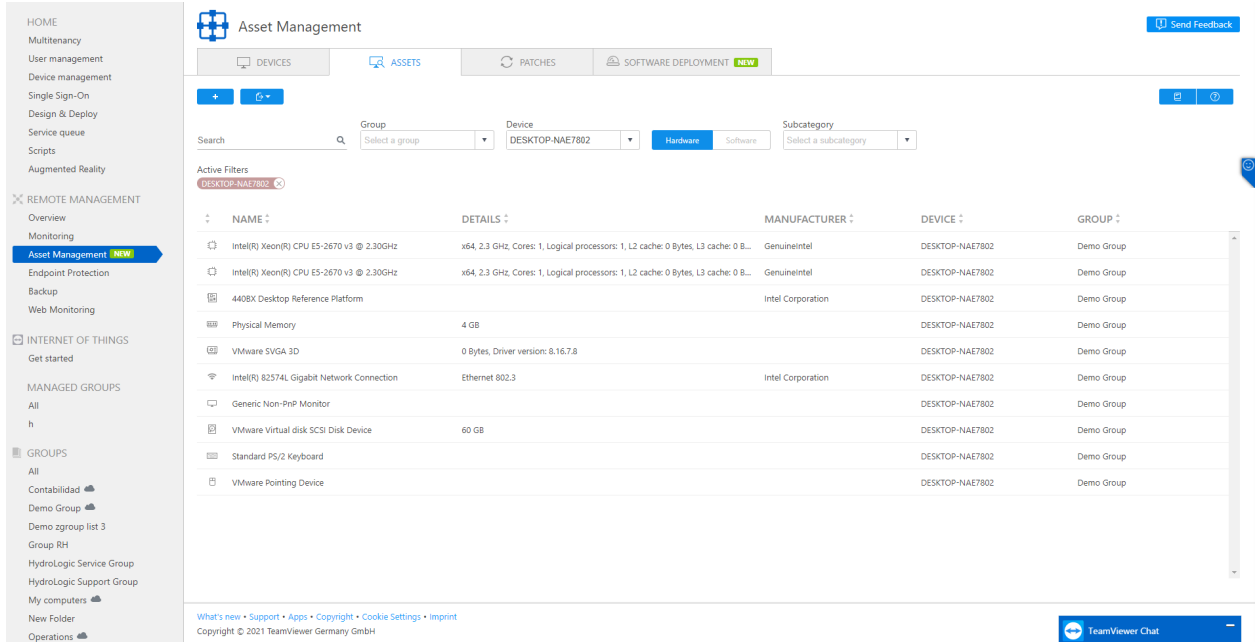


Image: Hardware Assets view within Asset Management.

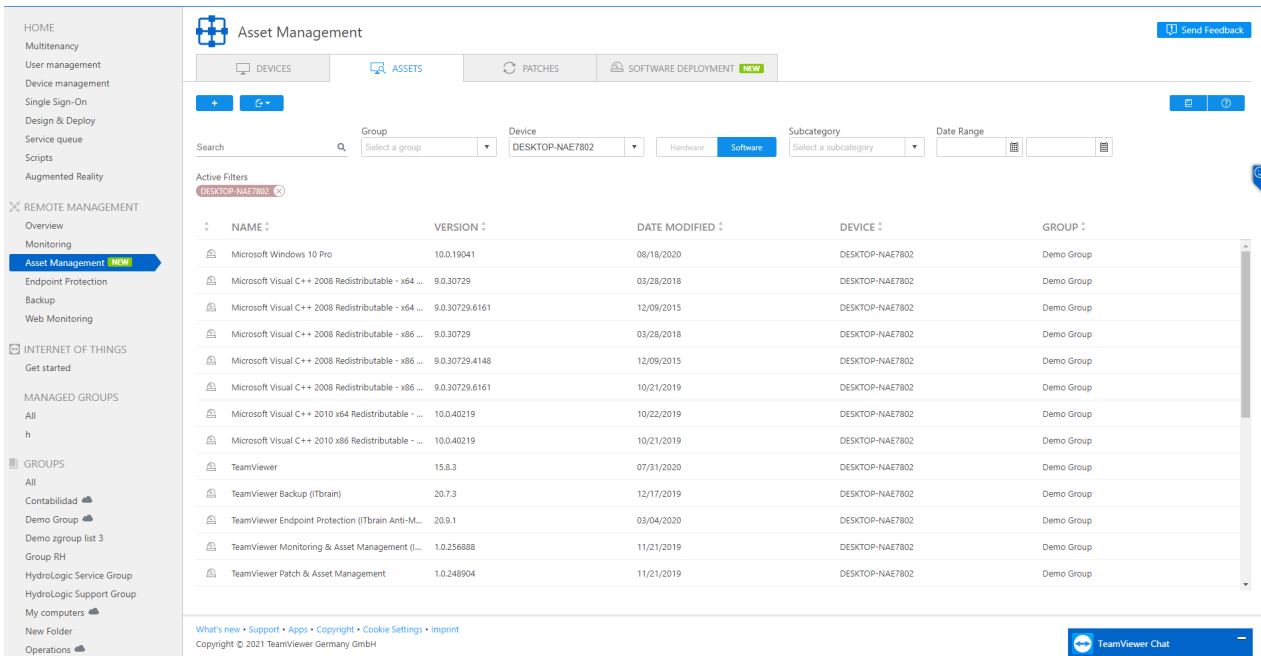


Image: Software Assets view within Asset Management

Report	Description
Software	Overview of applications installed on the devices, including the software version and date.
Updates	Overview of the installed Windows Updates including the date.
Hardware	Overview of installed hardware components, including Type , Name , and Manufacturer . This overview contains all reports listed below.
Processor	Overview of processors installed on the devices, including Name , Details , and Manufacturer .
Motherboard	Overview of motherboards installed on the devices, including Name , Details , and Manufacturer .
Physical Memory (RAM)	Overview of internal memory installed on the devices, including Name , Details and Manufacturer .
Disk Drive	Overview of hard drives installed on the devices, including Name , Details , and Manufacturer .
Optical Drive	Overview of input devices connected to the computers, (including Name , Details , and Manufacturer).
Video Controller	Overview of graphics cards installed on the devices, including Name , Details , and Manufacturer .
Network	Overview of network cards installed on the devices, including Name , Details , and Manufacturer .
Keyboard	Overview of keyboards connected to the devices, including Name , Details , and Manufacturer .
Pointing Device	Overview of input devices connected to the computers, including Name , Details , and Manufacturer .

4.11.3. Patch View

From the Patch view you can see detailed information about missing OS and 3rd party patches for your devices.

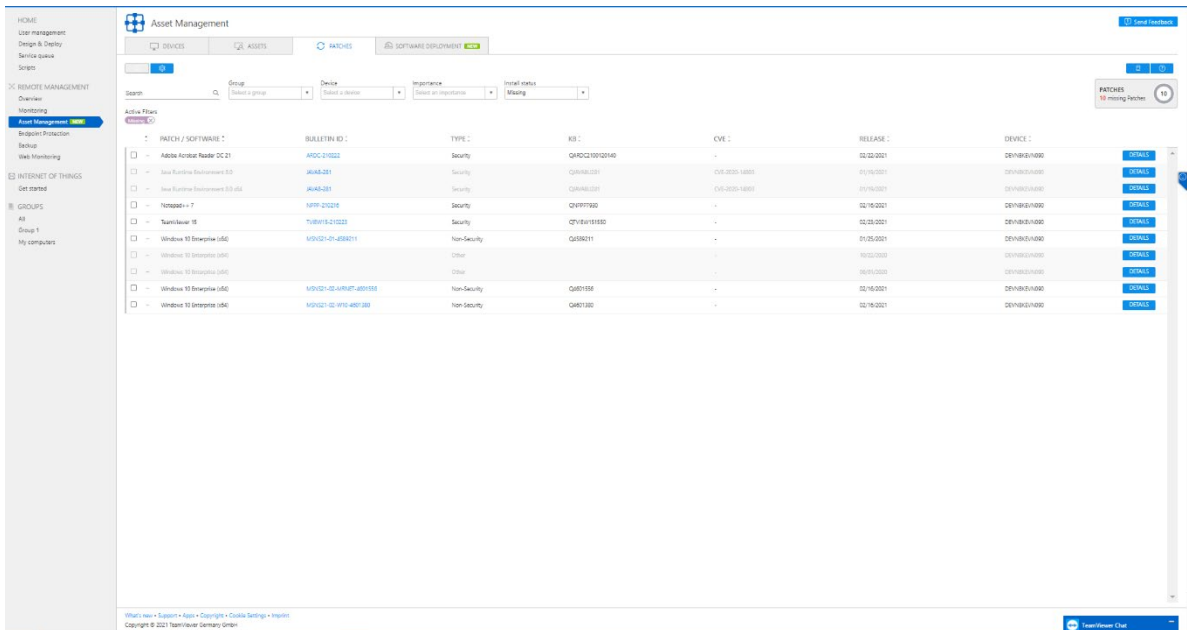


Image: Patch view within Asset Management

Each individual patch has the below described fields:

Severity icon: This field shows the importance of the patch -> Critical, Important, Low, Not rated.

Patch/Software: Here you can see the patch name and version for some patches

Bulletin ID: The Patch ID provided by the vendor. The ID is also a link to the changelog which is provided by each software vendor.

Type: This field shows if the patch is security or non-security (this information is coming from the Software Vendor)

KB: This is the knowledge base article number

CVE: This field contains all Common Vulnerabilities and Exposures which are related to the patch

Release: Here you can see when each patch was released

Device: This field displays the device name on which the patch is missing. In case there are more devices which have the same patch missing, instead of the device name you will see the number of devices which are affected.

Details: The button after clicking on which you will see some short notes from the vendor and patch size.

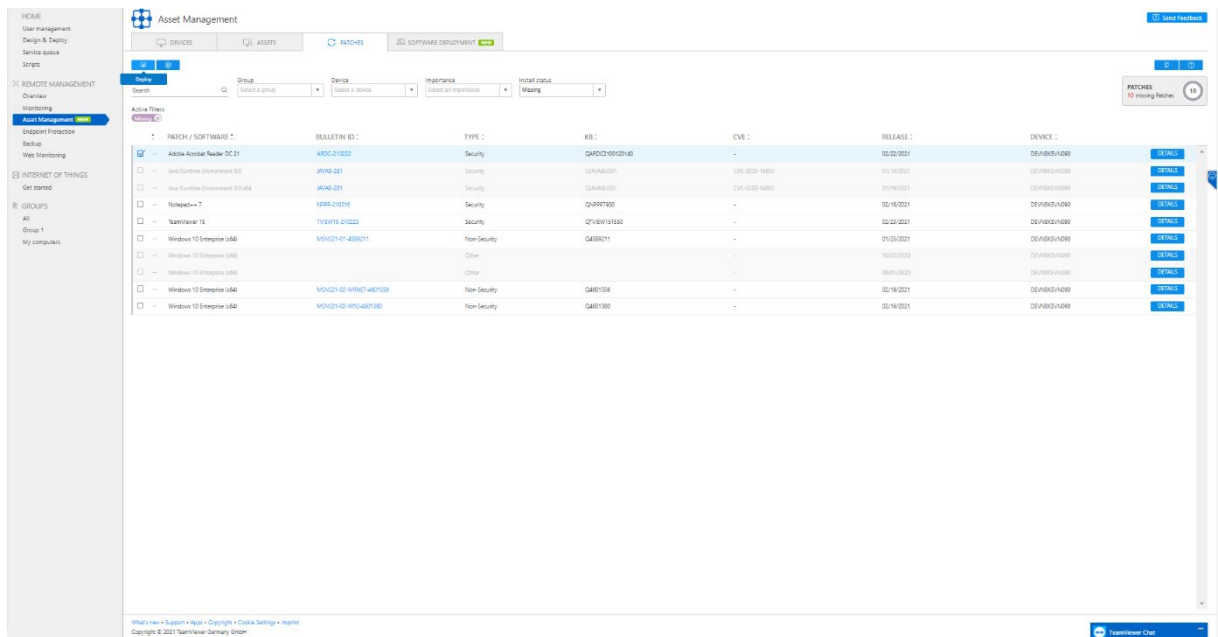


Image: Deploy Patch within Patch View

In the Patch view within Asset Management you can select a patch or multiple patches and deploy the selected patches to one or multiple devices. After selecting a patch, you just need to press on the deploy button.

The Patch view allows you to filter missing patches by:

- Group
- Device
- Importance
- Install status (here you can also see previews of installed patches)

Deployment of patches are possible only for online devices.

In the Patch view you can see some patches which are not possible to select, the row is greyed out with this tooltip: “This patch cannot be deployed remotely. Please Connect to the device and patch it manually.” It means that the patches require some additional action on the device side, e.g. captcha, additional authentication, accept EULA etc.

4.11.4. Patch Management Policy

Patch Management allows you to set predefined criteria based on which the system will trigger automatic patch deployment. A default Patch Management policy is an empty policy without any action. You can edit and change settings and conditions in the patch management policies at any time.

In Asset Management, under the “Device” tab, users can now see a policy section. Here, users can define and select policies for automatic patch deployment.

In the Patch Management Policy window, users can create new policies and delete or edit existing ones. From the 3 dots menu, users can duplicate policies. For creating a new policy, users need to click the “+” button on the right-hand bottom side. After creating a new policy, users will see the menu displayed below.

The policy should have a name (this is a mandatory field) and each policy can contain up to 5 conditions. In each condition, users can set the necessary criteria and schedule for automatic patch deployment. Each condition has several fields which need to be filled in order to be able to save the condition. These fields are:

- **Software vendor severity**
 - (Critical, Important, Low, Not Rated)
- **Patch classification**
 - OS Patches
 - 3rd Party Patches
- **Patch Type**
 - Security
 - Non-Security
- **Scheduled time for deployment.**
 - Daily
 - Weekly
 - Monthly
 - When available

Creating a policy without any defined conditions will not trigger any actions.

After adding the required conditions and assigning policies to devices, the system will automatically check the set conditions, and will trigger the deployment for those patches which comply with the predefined conditions.

Note: In cases where the automatically scheduled deployment cannot be done (e.g. device will be offline) deployment will be triggered automatically only when the device status change occurs within the two-hour window after the scheduled time. If the time period between scheduled time and status change is more than two hours, no action will be triggered, and the policy will be checked against the criteria during the next scheduled date.

4.11.5. Software Deployment

When the user activates the Monitoring and Asset Management license, he also receives access to the Software Deployment feature.

The Software Deployment feature enables you to remotely deploy the desired software on all available devices with in a few simple steps.

You can choose your desired software from a list of 300+ different software options and deploy them on multiple devices within a few clicks during the same deployment process.

Note: The Patch Management service should be active on the connected devices in order to see the device in the list.

In the Software Deployment view, this is the software deployment flow.

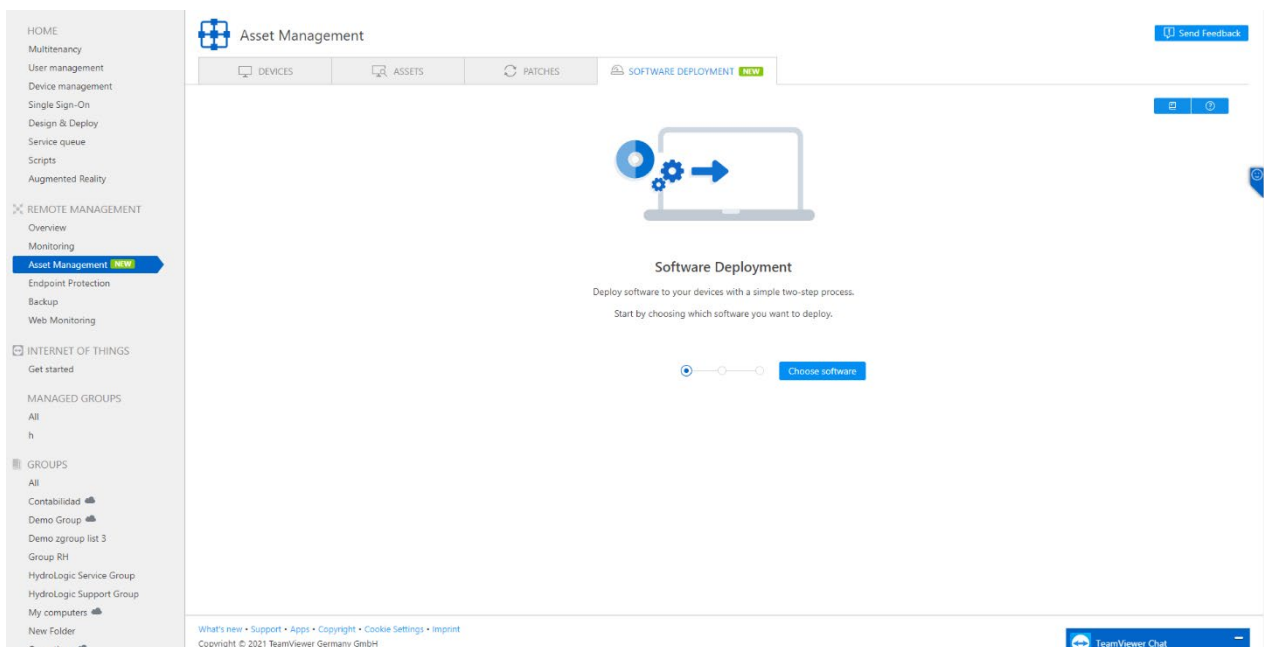


Image: Software Deployment Flow

Step 1: Select the software.

Choose the software that you want to deploy.

Search

SOFTWARE ↕	FILE NAME ↕	RELEASE ↕	SIZE ↕
<input type="checkbox"/> .NET 2.0 Redistributable Framework	dotnetfx_2_0.exe	06/21/2017	22.42 MB
<input type="checkbox"/> .NET Framework 4.8.3928.0	ndp48-x86-x64-allos-v2.exe	09/12/2019	111.94 MB
<input type="checkbox"/> 7-Zip 19.00	7z1900.msi	06/15/2020	1.3 MB
<input type="checkbox"/> 7-Zip 19.00	7z1900-x64.msi	06/15/2020	1.66 MB
<input type="checkbox"/> Adobe Acrobat Reader DC Classic 17.008.30051	AcroRdr20171700830051_MUI.exe	06/19/2020	178.39 MB
<input type="checkbox"/> Adobe Acrobat Reader DC July 2020 (Classic Tr...	AcroRdr20202000130002_MUI.exe	02/16/2021	224.21 MB
<input type="checkbox"/> Adobe Acrobat Reader DC May 2018 (18.011.2...	AcroRdrDC1801120040.exe	06/19/2020	115.05 MB
<input type="checkbox"/> Adobe Acrobat Reader Document Cloud 15.00...	AcroRdrDC1500720033_en_US.msi	11/21/2017	60.11 MB
<input type="checkbox"/> Adobe Acrobat Reader Document Cloud 15.00...	AcroRdrDC1500720033_MUI.exe	11/21/2017	146.89 MB

Image: Software Selection View

Step 1: Firstly, you need to select the software that you want to deploy. You can select a single software or multiple software to deploy.

The software list view allows you to filter the available software by:

- Manual Search

The software list view allows you to sort available software by:

- Software Name
- File Name
- Release Date
- Size

Step 2: Select the devices.

Choose the devices that you would like to deploy the software on.

Note: If you would like to deploy software on your devices, please make sure that Monitoring & Asset Management (including Patch Management) service is active.

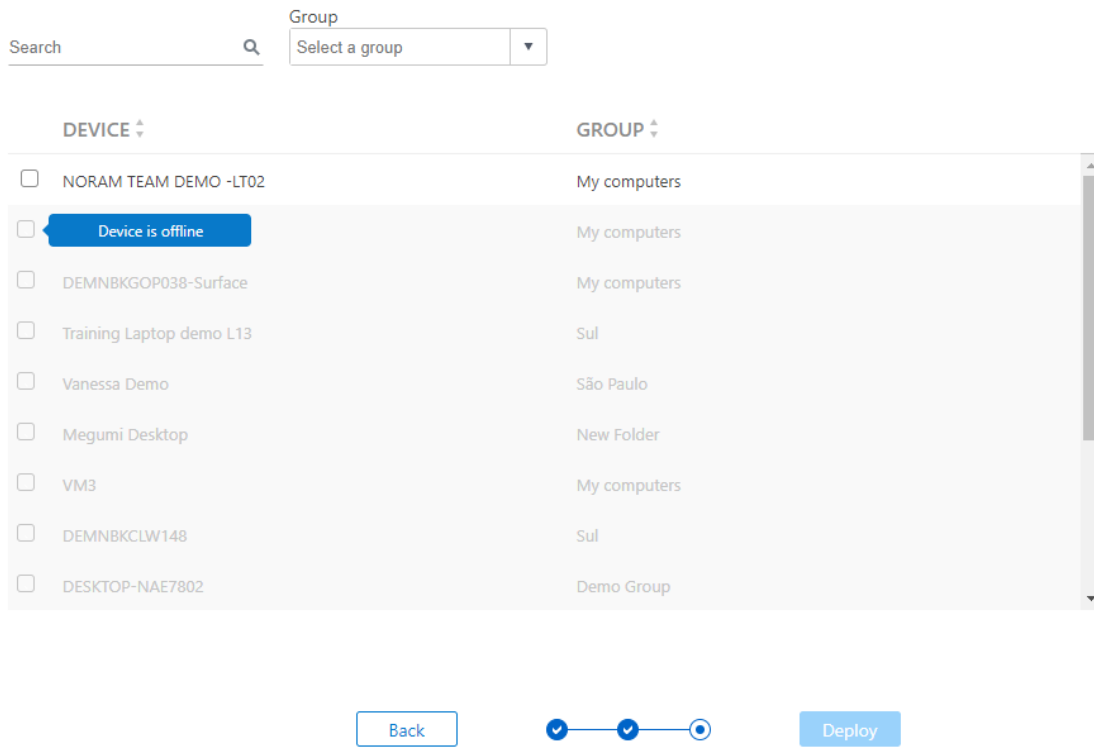


Image: Device Selection View with online and offline Devices

Step 2: During the second step you need to select the devices that you want to deploy the selected software on. Software deployment is only possible on those devices that are online and have active an Patch Management Service.

The devices which are offline will be in a disabled state.

The device list view allows you to filter available devices by:

- Manual Search
- Group
- Device

Step 2: Select the devices.

Choose the devices that you would like to deploy the software on.

Note: If you would like to deploy software on your devices, please make sure that Monitoring & Asset Management (including Patch Management) service is active.

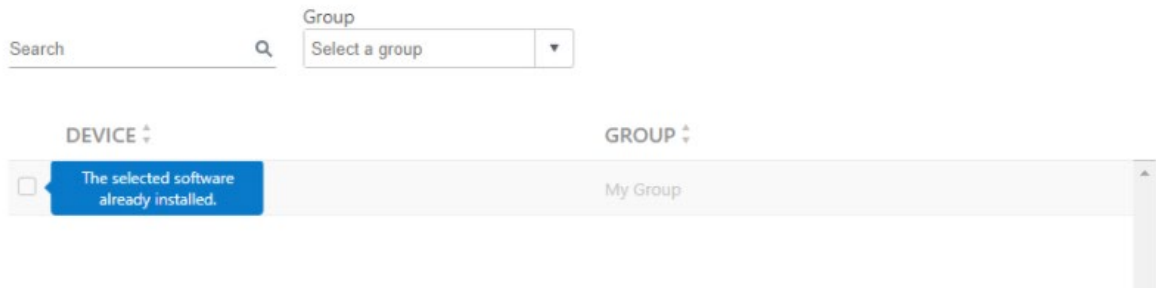


Image: All software installed view

In this view all the selected software has already been deployed on the given device, and the deployment is not possible.

Step 2: Select the devices.

Choose the devices that you would like to deploy the software on.

Note: If you would like to deploy software on your devices, please make sure that Monitoring & Asset Management (including Patch Management) service is active.

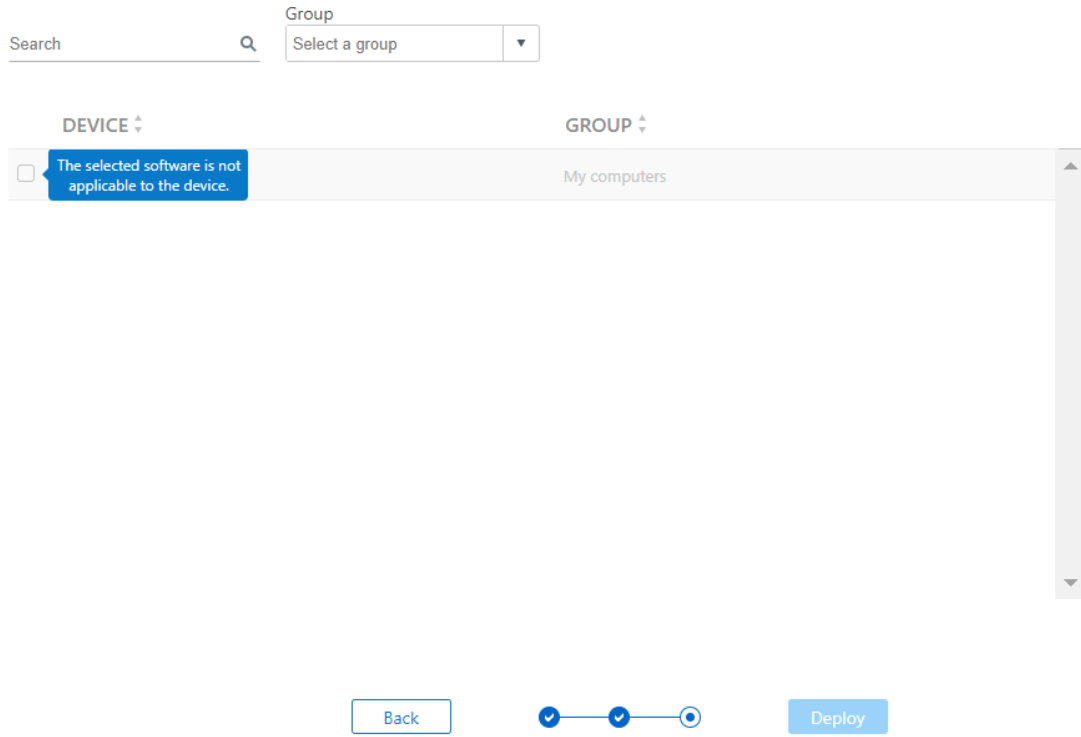


Image: Software and Device not applicable state view

This view shows that the software is not applicable with the selected device. This means that there are either technical incompatibilities or a better version that would be more suitable technically is available.

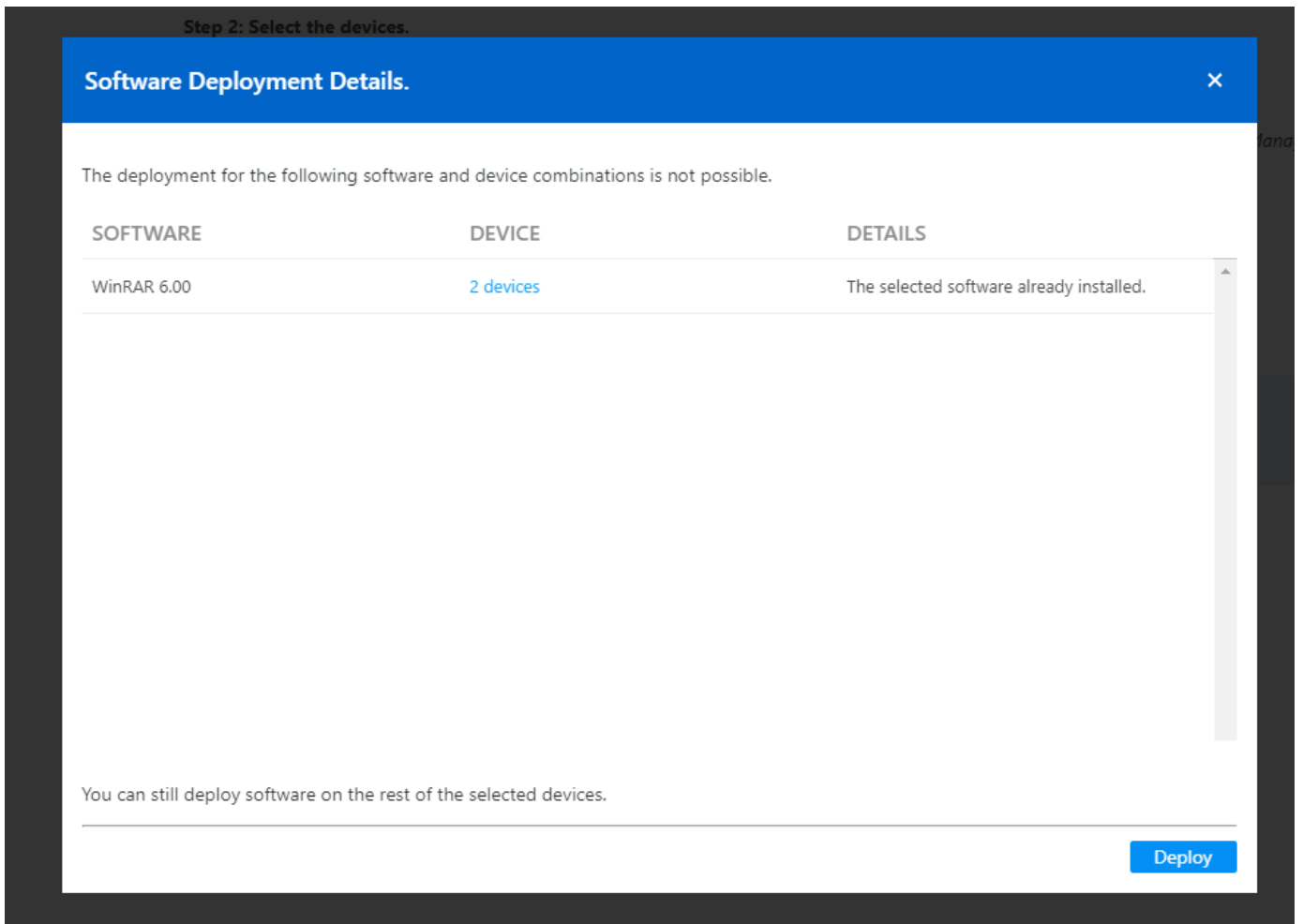


Image: Software and Device incompatibility view

This view shows that some of the software have already been deployed on the device and therefore the deployment is not possible.

However, the deployment for the rest of the selected software and devices will be started when clicking on the “Deploy” button.

A user will not see any info pop-ups if there aren’t any software and device conflicts and will be redirected to the first page in the flow.

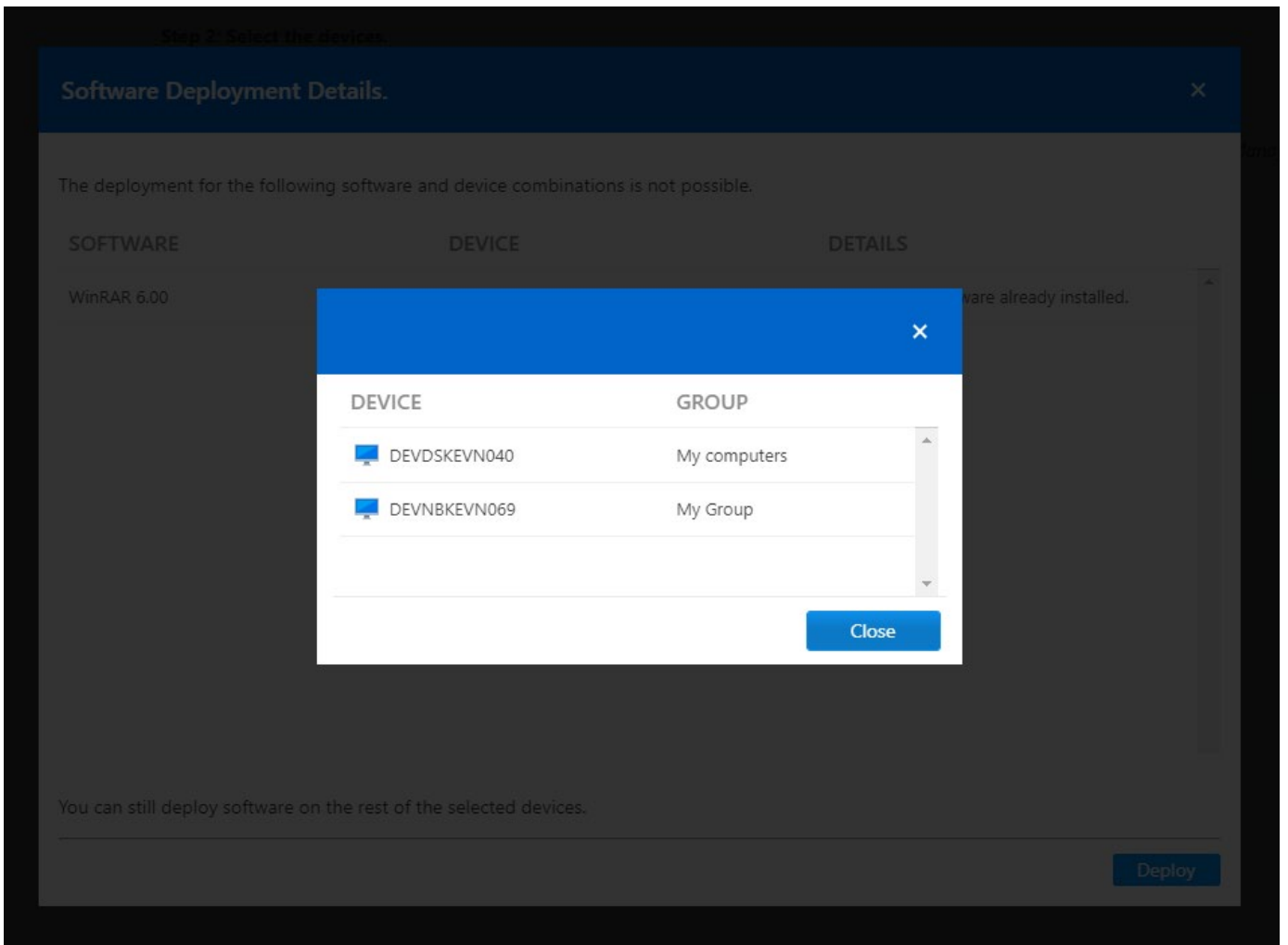


Image: List of Incompatible Devices View

When clicking on the device info, you will see the list of devices that already have the software installed on. This means that the deployment process will not affect those devices.

After clicking on the "Deploy" button, you will be redirected to the History Logs table, where you will see the list of deployed software and devices.

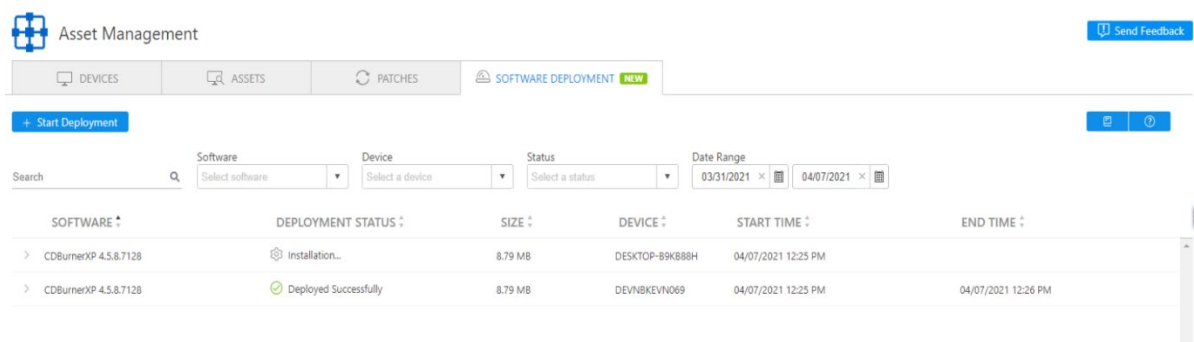
4.12. Software Deployment History Logs

After finishing the deployment process, you will be redirected to the History Logs table., where you can either track the current status of the deployment processes or start a new deployment.

You have all the software deployment information centralized in one table view. In history logs table you will be able to track the software deployment cycle, with all the detailed information about when and on which device the software has been rolled out.

Within the History Logs you will be able to see;

- The current status of your deployment
- When the Software Package was deployed on a given device
- The length of the deployment from download to installation for each deployment
- Check the status of your device to make sure whether a reboot is needed after software deployment



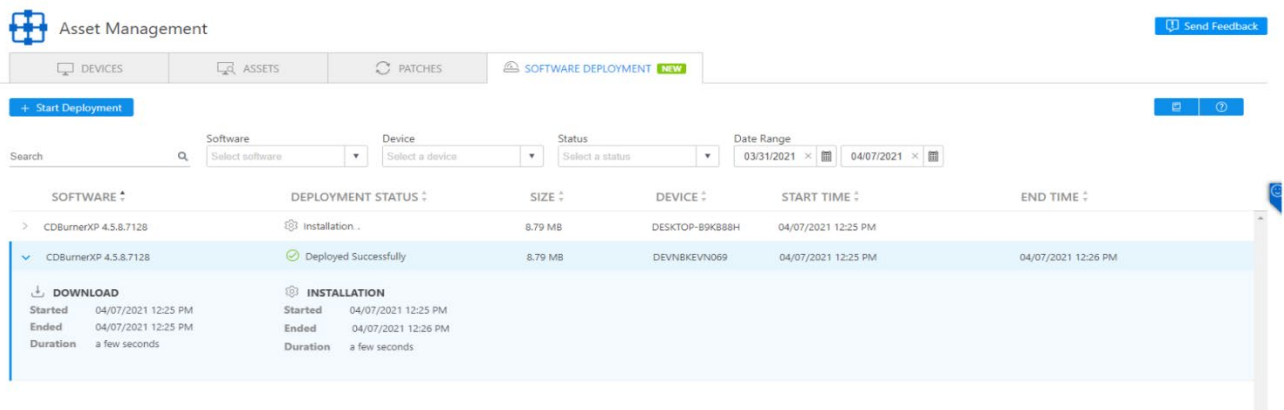
The screenshot shows the 'Asset Management' interface with the 'SOFTWARE DEPLOYMENT' tab selected. A table displays deployment history for 'CDBurnerXP 4.5.8.7128'. The table has columns for Software, Deployment Status, Size, Device, Start Time, and End Time. Two rows are visible: one with 'Installation...' status and another with 'Deployed Successfully' status.

SOFTWARE	DEPLOYMENT STATUS	SIZE	DEVICE	START TIME	END TIME
> CDBurnerXP 4.5.8.7128	⚙️ Installation...	8.79 MB	DESKTOP-89K888H	04/07/2021 12:25 PM	
> CDBurnerXP 4.5.8.7128	✅ Deployed Successfully	8.79 MB	DEVNBKEVN069	04/07/2021 12:25 PM	04/07/2021 12:26 PM

Image: Software Deployment Status Overview

In the Software Deployment History Logs table, you will be able to see the following details:

- Software Name
- Deployment Status
- Software Size
- Device ID
- Deployment Start Time
- Deployment End Time



The screenshot shows the same table as above, but with the 'Deployed Successfully' row expanded. It provides detailed information for both the 'DOWNLOAD' and 'INSTALLATION' phases, including start and end times and durations.

SOFTWARE	DEPLOYMENT STATUS	SIZE	DEVICE	START TIME	END TIME
> CDBurnerXP 4.5.8.7128	⚙️ Installation...	8.79 MB	DESKTOP-89K888H	04/07/2021 12:25 PM	
✓ CDBurnerXP 4.5.8.7128	✅ Deployed Successfully	8.79 MB	DEVNBKEVN069	04/07/2021 12:25 PM	04/07/2021 12:26 PM

DOWNLOAD		INSTALLATION	
Started	04/07/2021 12:25 PM	Started	04/07/2021 12:25 PM
Ended	04/07/2021 12:25 PM	Ended	04/07/2021 12:26 PM
Duration	a few seconds	Duration	a few seconds

Image: Software Deployment Status Expanded View

For additional details, you can expand the row to find all the relevant information for the Download and Installation Processes.

To give flexibility to adjust the reports based on the user needs, we have the following filters available:

- Software
- Device
- Status
- Deployment date range

Now, when you have successfully deployed the software, you can keep them up to date with our Patch functionality.

4.13. Asset and Patch Management API

Our web-based API allows you to access data and control various aspects of their TeamViewer account. You can use the API to develop apps that integrate TeamViewer functionality into your own corporate environment or can develop apps that everyone can use.

The API uses REST to communicate with the application and the secure authorization standard OAuth 2.0 to manage access to data.

For more details see the [Develop Custom TeamViewer Solutions](#) web page and the API

Documentation - <https://webapi.teamviewer.com/api/v1/docs/index#/>

Patch Management Policy Management

Show/Hide | List Operations | Expand Operations

GET	/api/v1/PatchManagement/Policy	Get Patch Management Policies - action is used to get the list of Patch Management policies
GET	/api/v1/PatchManagement/Policy/{id}	Get Patch Management Policy - action is used to get the details of the Patch Management Policy
POST	/api/v1/PatchManagement/Policy/Assign	Post Patch Management Policies - action is used for updating assigned Patch Management Policies

PatchManagement

Show/Hide | List Operations | Expand Operations

GET	/api/v1/patchmanagement/devices	
-----	---------------------------------	--

- GET /api/v1/PatchManagement/Policy - action is used to get the list of Patch Management policies
- GET /api/v1/PatchManagement/Policy/{id} - action is used to get the details of the Patch Management Policy
- POST /api/v1/PatchManagement/Policy/Assign - action is used for updating assigned Patch Management Policies
- GET /api/v1/patchmanagement/devices - action is used to get the service activation information
- POST /api/v1/Monitoring/devices - Activate action is used for activating patch management and monitoring services on a managed device.
- For more information – see the API documentation

5. Endpoint Protection and Endpoint Detection and Response – powered by Malwarebytes

To protect your devices against malware, ransomware, and more, use one of our **Endpoint Protection solutions – powered by Malwarebytes and integrated into TeamViewer.**

5.1. Requirements

5.1.1. Operating System requirements for Malwarebytes Endpoint Protection

- TeamViewer client: Remote Control or Host, version 15.19 or newer
- Windows Server†: 2019, 2016, 2012, 2012 R2, SBS 2011, 2008 R2 SP1‡§
- Windows: 10, 8.1, 8, 7§, XP SP3**
- Mac: OS X 10.11 El Capitan, macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1/11.2 Big Sur
- Linux: Debian 8, Debian 9, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 15, Ubuntu 20, Ubuntu 18, Ubuntu 16, other RPM-based distros
- TeamViewer client: Host, version 15.21 or newer

5.1.2. Operating System requirements for Malwarebytes Endpoint Detection and Response

- Windows Server†: 2019, 2016, 2012, 2012 R2, 2008 R2 SP1‡§
- Windows: 10, 8.1, 8, 7 SP1§
- Mac: macOS 10.13 High Sierra, macOS 10.14 Mojave, macOS 10.15 Catalina, macOS 11.1, 11.2 Big Sur

5.1.3. Windows hardware requirements

- CPU: 1 GHz*
- Disk space: 100 MB (program + logs)
- RAM: 1 GB (client); 2 GB (server)
- Network: Active Internet connection

5.1.4. Apple hardware supported

- Apple computers running Intel core processors
- Apple computers running Apple's M1 chip.

5.1.5. Operating system annotations

- † Excludes Server Core installation option
- ‡ Microsoft™ patch KB3140245 must be installed for 2008 R2 SP1.
- § For Windows 7 or Windows Server 2008 R2 devices, you need to apply the Microsoft 2019-09 Security Update. For more information, see Windows 2019-09 Security Update for Windows devices running Malwarebytes business products.
- * Advanced RISC Machines (ARM) processors are not supported
- ** 32-bit only

Notes

- .NET 4.5.2 or 4.6 must be installed and enabled on Windows systems.
- Behavior Protection features are only supported on endpoints using Windows 7 and newer.
- Server or workstation subscriptions are required to enable features for these endpoints.

Malwarebytes Nebula link: System requirements for Malwarebytes Nebula

5.1.6. Network access and Firewall settings requirements

- TeamViewer Remote Control and Host application Port 443
- whitelist if possible: *.teamviewer.com
- Transport Layer Security (TLS) 1.2 must be enabled for all endpoints.
- Domains to exclude For communication flow from the device to Malwarebytes cloud:
 - <https://ark.mwbsys.com>; <https://blitz.mb-cosmos.com>; <https://cdn.mwbsys.com>;
<https://cloud.malwarebytes.com>; <https://data-cdn.mbamupdates.com>; <https://data-cdn-static.mbamupdates.com>; <https://detect-remediate.cloud.malwarebytes.com>;
<https://hubble.mb-cosmos.com> ; <https://keystone-akamai.mwbsys.com>;
<https://keystone.mwbsys.com> ; <https://nebula-agent-installers-mb-prod.s3.amazonaws.com>;
<https://nebula-diagnostics-mb-prod.s3.amazonaws.com>
<https://nebula-helix-syslog-mb-prod.s3.amazonaws.com>; <https://sirius.mwbsys.com> ;
<https://socket.cloud.malwarebytes.com> ; <https://storage.gra.cloud.ovh.net>;
<https://telemetry.malwarebytes.com>
<https://downloads.malwarebytes.com>; <https://links.malwarebytes.com>;
<https://download.toolslib.net>; <https://meps.mwbsys.com>

Malwarebytes Nebula link: Network access requirements and firewall settings for Malwarebytes Nebula

5.2. Licensing

Malwarebytes Endpoint Protection and Endpoint Detections and Response licenses are purchased separately from TeamViewer Remote Control licenses.

The licenses are split between Workstations and Servers. Any license can be purchased separately based on the current needs.

5 endpoints are equal to 5 devices, and counting is done after the activation of the product on the device.

- Endpoint Protection Workstation license
- Endpoint Protection Server license
- Endpoint Detection and Response Workstation
- Endpoint Protection and Response Server

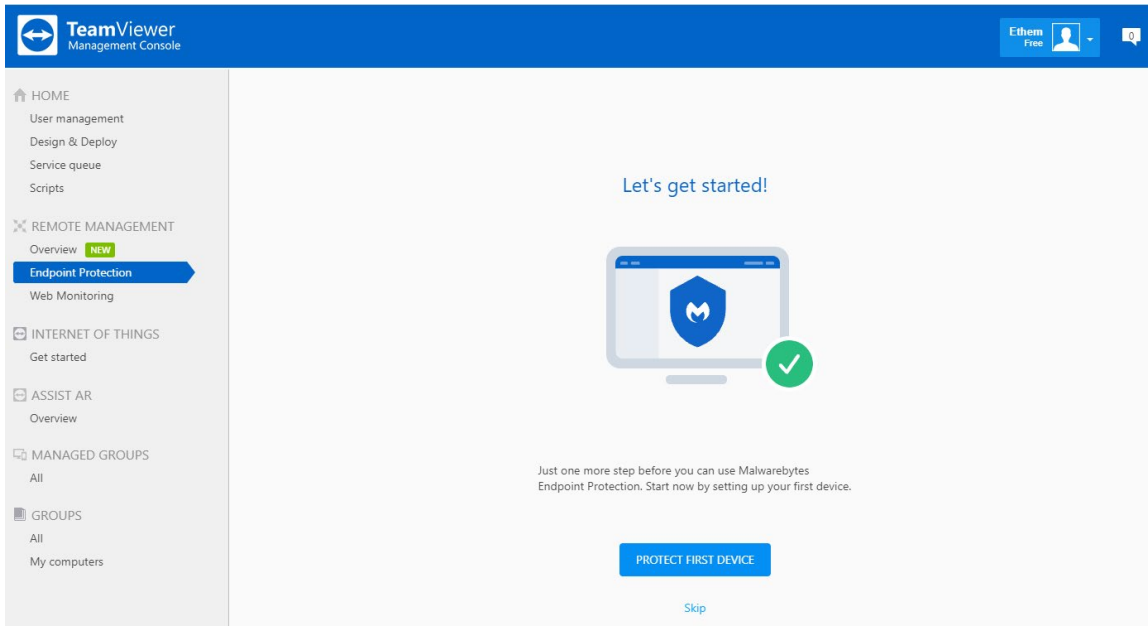
Note: Linux activations are always counted towards a server license.

Note: Server licenses unlock more advanced settings specifically designed for server operations.

5.2.1.Activation

After you purchase a Malwarebytes license, you'll receive a confirmation email. Click on the activation link in the email to activate the license for your TeamViewer account.

Once you have activated the license, it will automatically be linked to your TeamViewer account and will be ready for immediate use.



Note: If you set up your TeamViewer account under a company profile, the TeamViewer Remote Management license will be part of the company profile and all users with permission will be able to manage the Remote Management services.

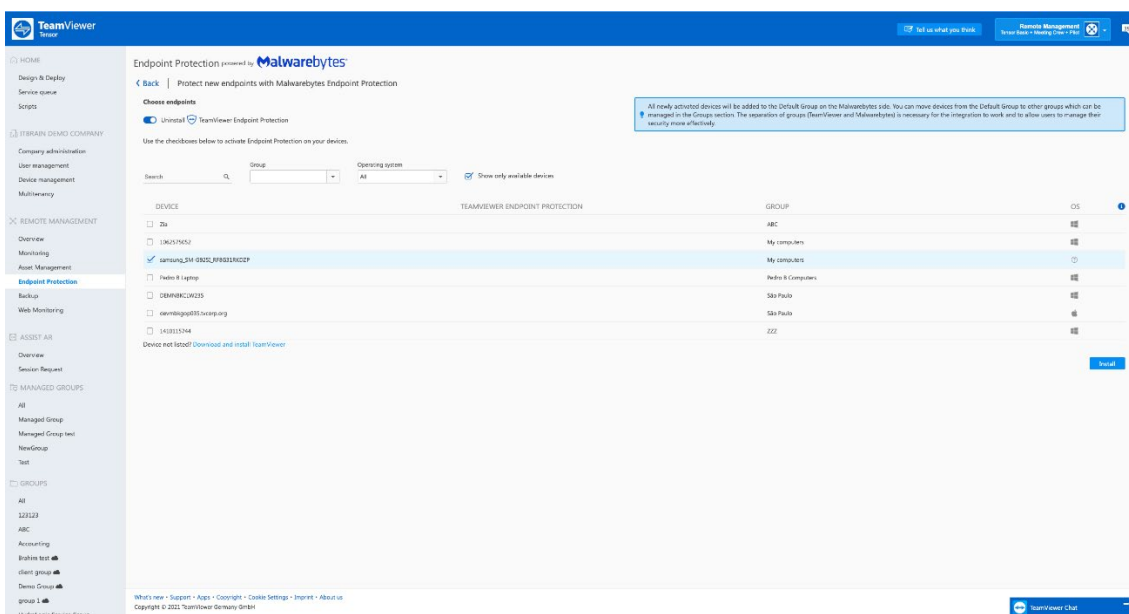
Note: All four paid license types (Endpoint Protection for Workstations, Endpoint Protection for Servers, Endpoint Detection and Response for Workstations, Endpoint Detection and Response for Servers) can be activated on the same account/company profile. It is not possible to activate two licenses of the same type on one account, e.g., one Endpoint Protection license with 10 endpoints and another one with 15 endpoints.

Note: Only a TeamViewer Management Console administrator can activate a license for the company profile. Standard accounts are not bound to this restriction.

Note: Only one license can be activated per product. If a prior Malwarebytes license is linked to the email address, which is also used for the TeamViewer login, then a request to delete the former Malwarebytes account will be necessary, and our support can help here.

- Endpoint Protection and Endpoint Detection and Response can be activated from the TeamViewer Management Console, Endpoint Protection Tab.
- The application installed on the targeted device is the same for both products. Endpoint Detection and Response features can be unlocked via the policy if a license is presented on the account.

- During the initial setup, the first device activation page will ask you to select the first device to activate Endpoint protection on. After the initial setup, the activation of new devices can be done from the Device View → "+" Button.
- All newly activated devices (installed on a device) will be shown in the Default Group.
- Devices that are not compatible/not supported will not appear by default in the list. If you uncheck the "show only available devices", devices that are not available will show up in grey. Also, the reason why they are not available will be displayed in the info bubble on the right side of the grid.
- When devices are selected to be installed, the progress moves to the Devices View and statuses(activation in progress, device protected and activation failed) appear.
- If activation fails, meaning that the installation process did not complete for a reason, the appropriate message, including the specific reason, will be shown when hovering over action on the failed message.



5.3. Product pages and views

Malwarebytes Endpoint Protection and Malwarebytes Endpoint Detection and Response are located in the TeamViewer Management Console, under the Remote Management pane on the left side of the console.

5.3.1. Dashboard view

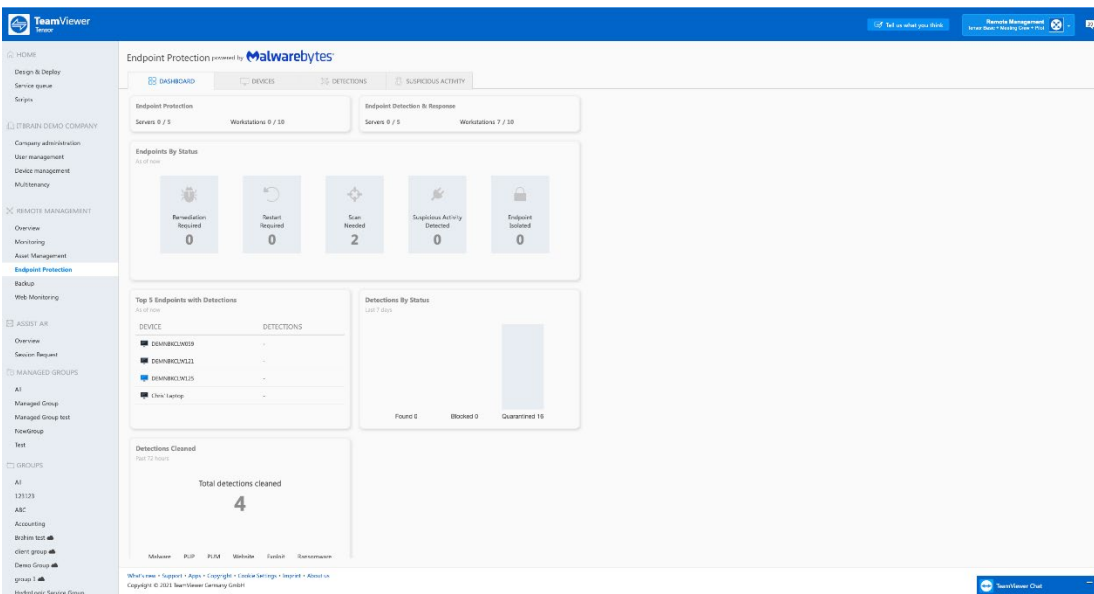
The dashboard view is the default page for both products, and it will be loaded first at every login. We provide several tiles for a glance status view so that the technicians will be able to know what is happening with the deployed fleet at login.

- **License tiles**
 - Show the licenses statuses, used endpoints vs. available endpoints and the breakdown between workstations and servers
 - Endpoint Protection
 - Endpoint Detection and Response

- **Endpoints by status tile**
 - Remediation required
 - Displays the number of devices that have detections found with remediation required status.
 - Restart required
 - Displays the number of devices that have the status: Restart required
 - Scan needed
 - Displays the number of devices that have the status: Scan needed
 - Suspicious Activity detected status (Endpoint Detection and Response only)
 - Displays the number of devices that have Suspicious activities found
 - Endpoint Isolated status (Endpoint Detection and Response only)
 - Displays the number of isolated devices

- **Top 5 Endpoints with Detections Tile**
 - Displays the top 5 devices with detections found

- **Detections by Status**
 - Displays the number of detections with the statuses:
 - Found
 - Blocked
 - Quarantined



5.3.2.Devices View

The devices view is the main management view for devices where statuses, controls and settings are being managed for the deployed fleet.

Devices grid

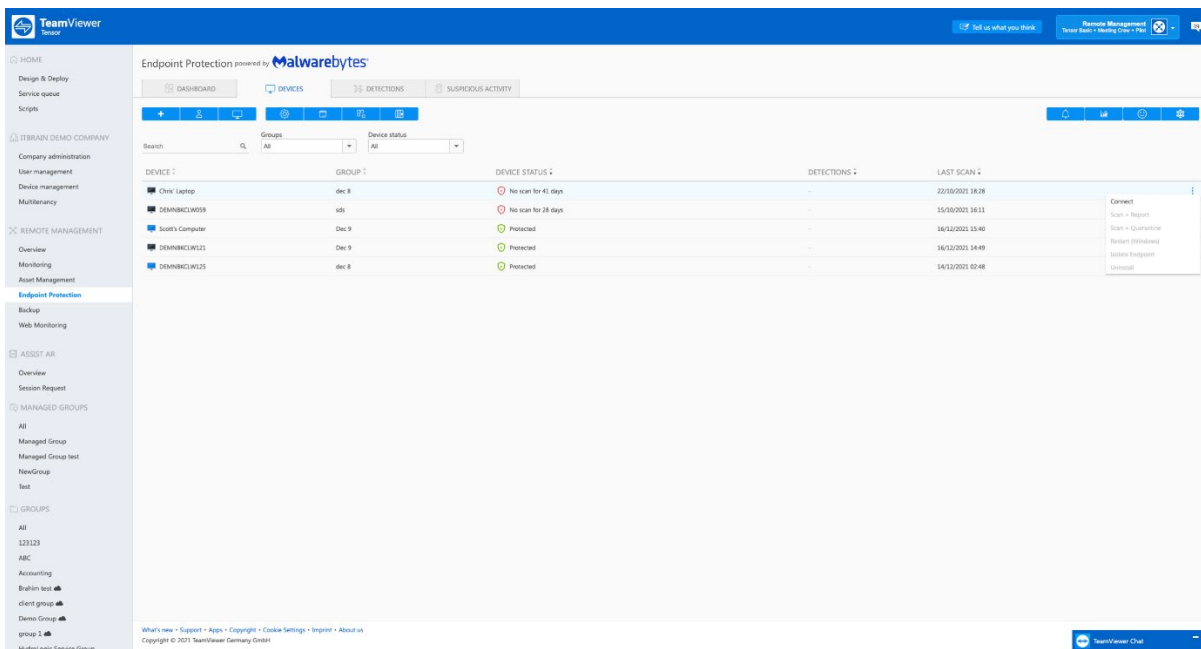
Shows the list of devices that have Endpoint Protection and Endpoint Detection and Response activated. We show the following parameters in the grid that help the technician to troubleshoot and manage their devices.

- **Device name**

- Shows the machine name as shown in the TeamViewer Computers and Contacts list in the Management Console.
 - The device name is the machine name in most cases (Windows, macOS, or Linux).
 - The device name can be changed, and the alias can be added to the Computers and Contacts list in the Management Console.
- **Groups**
 - Shows in which groups devices belong to.
 - The Malwarebytes groups shown in the device view are separate from TeamViewer groups.
 - All newly activated devices are being assigned to the "Default Group", then devices can be moved in different groups by the technicians.

Note: The separation between Malwarebytes and TeamViewer groups is necessary for the integration to work.

- **Device status**
 - Shows the latest status for the device
 - The statuses are prioritized in categories based on severity:
 - Red - high severity
 - Yellow - medium severity
 - White - ongoing task.
 - Green - good state, the device is protected
- **Detections**
 - Displays the number of detections found, remediation required, restart required state for each device.
 - The number for each device can be clicked and it will be forwarded to the user to the detections view with the necessary filters applied.
- **Last Scan**
 - Displays the last scan date of the device
 - This is important when the statuses are calculated and it allows the technician to see which devices are not getting scanned.
- **Hover over the menu (the vertical three dots)**
 - When hovering over any device row, the three-dots menu will appear on the right side of the row.
 - Connect action
 - Connects to the device via TeamViewer Remote Control
 - Scan+Report
 - Will send a scanning command to the device. Only the results will be reported as Detections found.
 - Scan+Quarantine
 - Will send a scanning command to the device and the results will be quarantined.



5.3.3. Detection View

The Detections view shows all detections for all devices over time. We keep detections for 90 days then they are deleted. The view shows time-series events for detections and statuses which happened on the devices.

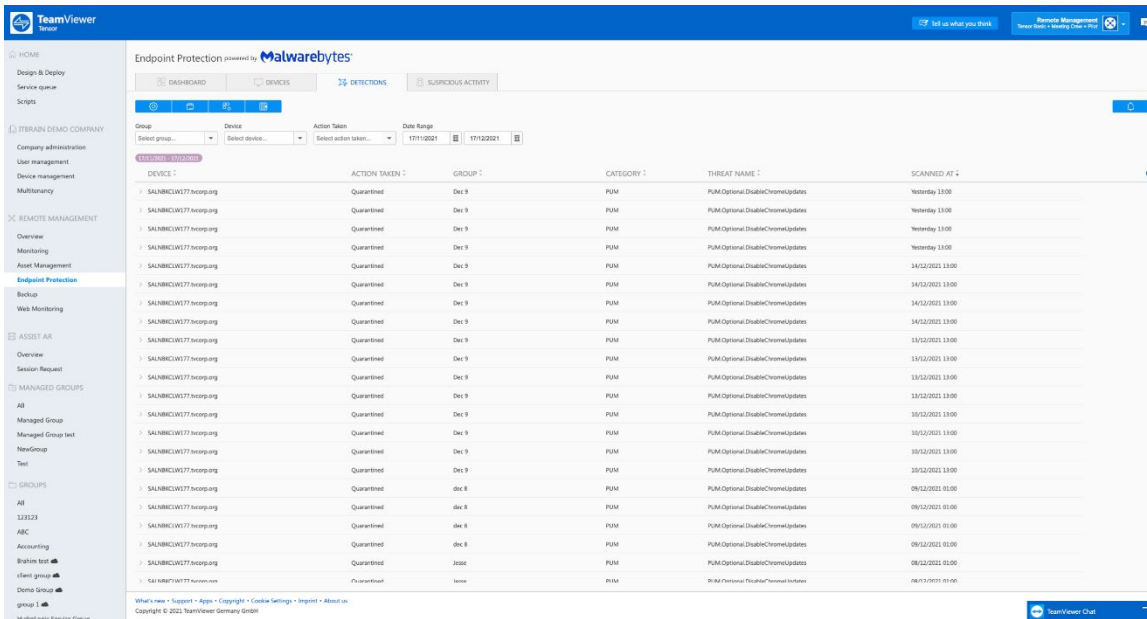
Detection filtering

The detections grid can be filtered by:

- Groups
- Device
- Action taken:
 - Blocked, Quarantined, Found, Deleted, Restored
- Date range

Detections operations

The only way to troubleshoot a detection is to quarantine it if it was found or to restore it from the quarantine if detection was falsely detected and quarantined.



Detection details

By clicking on an individual detection, the field will expand and more details about the detection will be shown. The information shown is useful for a deeper malware investigation.

- Location
 - Shows the full path on the device where the detection was found
- Category
 - Malware, PUP (Potentially unwanted Program), PUM (Potentially Unwanted Modification), Exploit, Ransomware, Remote intrusion, Website
- Type
 - Exploit, Extension, File, Folder, Inbound connection, Module, Outbound connection, Process, Registry key, Registry value.
- Reported at
 - When the detection was reported by the device to the cloud console



5.3.4.Suspicious Activity View

This view is unlocked for accounts that have The Endpoint Detection and Response license activated.

Suspicious activity filtering

The activities can be filtered by:

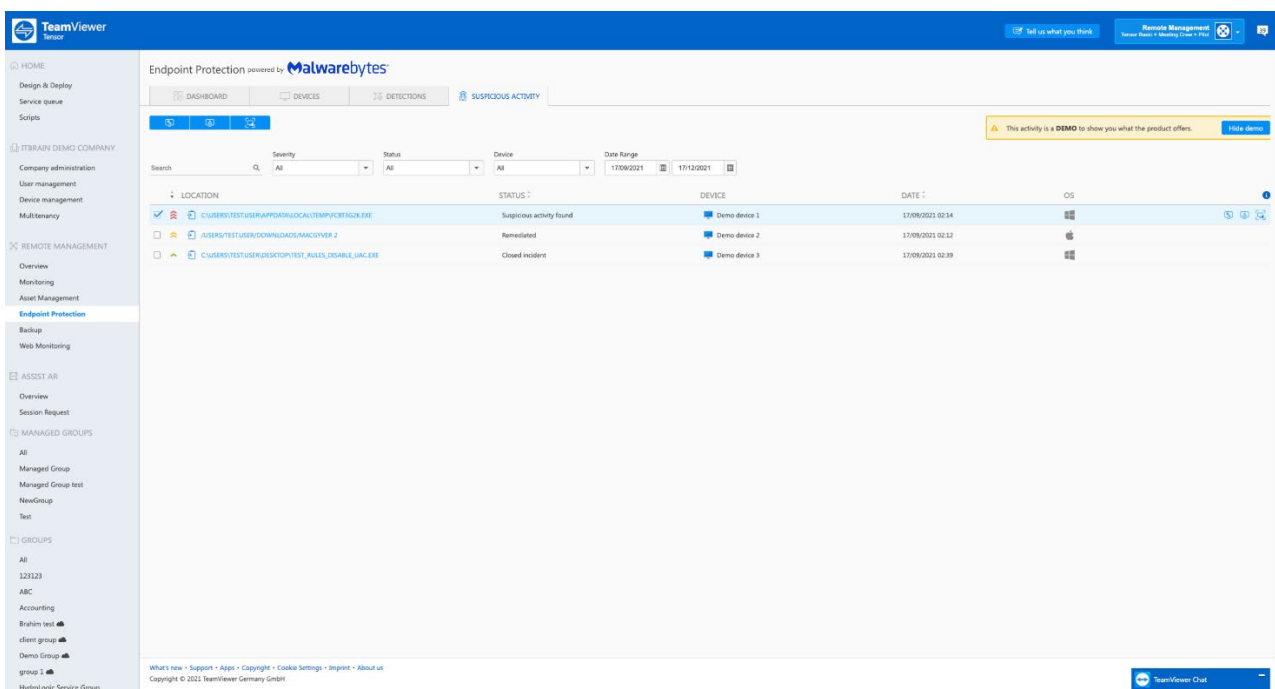
- Location
- Severity
 - Green - Low
 - Yellow - Medium
 - Red - High

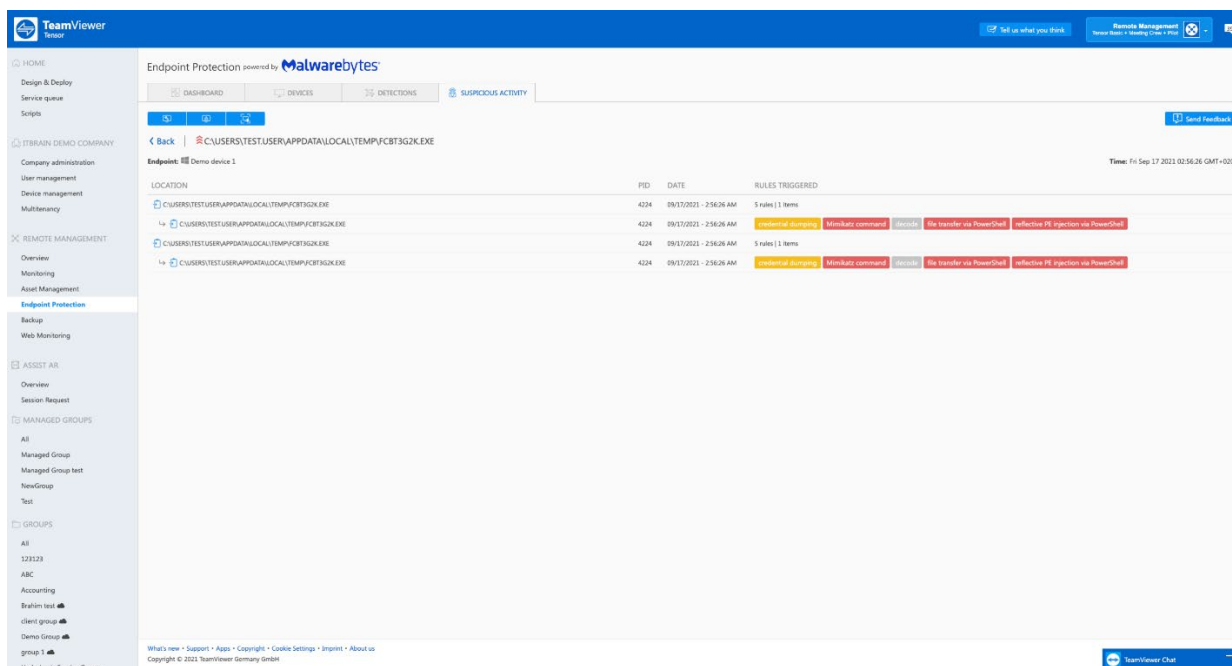
- Status
- Device
- Date range

Suspicious activities grid

Shows all suspicious activities with information relevant for the investigation by the technician

- Severity
 - Low
 - Medium
 - High
- Location
 - Shows the full path on the device where the suspicious activity was found
- Status
 - Shows the latest status for the suspicious activity
 - The statuses are important for the management and auditability working with the Suspicious activities
 - Suspicious activity found
 - Suspicious activity blocked
 - Pending remediation
 - Remediated
 - Closed incident
- Device
 - Shows the device name where the suspicious activity was found
- Date
 - Shows the time and date when the activity was reported
- OS
 - Shows the operating system of the device





Suspicious activity operations

When hovering over any detection row, the action buttons will appear:

- Remediate
 - Reverts back the malware and/or the actions which were deemed as harmful on the device.
 - If ransomware was recorded, it would roll back all encrypted files to a state before the ransomware attack.
- Close
 - This will close the incident. It has no effect on the device.
 - The close action is for traceability and auditability, which is important when working with security incidents.
- Isolate endpoint
 - This action will trigger an endpoint isolation task on the endpoint where the endpoint will be blocked for:
 - Desktop isolation
 - Network isolation
 - Process isolation

5.4. User Management

Malwarebytes Endpoint Protection user management is different than TeamViewer Management Console user management.

Malwarebytes user management is able to assign user roles to each user based on the criteria defined below:

5.4.1. User Roles

- Read-Only
 - The read-only user role can only view all information from assigned groups, generate reports, and set up email notifications.

- The "Default Group" is always assigned to all users.
- All new users added will be assigned by default the Read-Only user role
- **Manager**
 - The manager user role can view and edit assigned groups only.
 - The "Default Group" is always assigned to all users, including the Manager user role.
 - A Read-only user role be promoted to a Manager by the Administrator
- **Administrator**
 - Can operate any changes on the Malwarebytes deployed fleet and has access to all resources in Malwarebytes Nebula Console
 - Add new devices
 - Uninstall devices
 - Create, modify, and delete groups
 - Work with exclusions
 - Modify policies for all groups
 - Assign groups to "read-only" and "manager" user roles
 - Add new users, promote users, demote users
 - All TeamViewer Management Console Administrators and User Administrators will be Malwarebytes Administrators.
 - The administrator who activated the license will get the account set up automatically. The subsequent administrators in the TeamViewer company profile will be able to create an on-demand account for Malwarebytes at first login.
 - Example:
 - Admin 1 purchases and activates a Malwarebytes Endpoint Protection license on the TeamViewer Management Console.
 - Admin 2 will log in and he will be asked to click on get started in order for the account to be created by clicking on the Endpoint Protection tab in the TeamViewer Management Console.
 - Both Admin 1 and 2 will have the Administrator role on the Malwarebytes Nebula and will be able to operate the same changes to the product.
 - Administrators can add new users to the Malwarebytes user management list by selecting from a list of all TeamViewer Company profile users.

Feature	Administrator	Manager*	Read-Only*
Endpoint Protection			
Add users	✓	✗	✗
Edit Groups	✓	✗	✗
Edit Users	✓	✗	✗
Activate Endpoints	✓	✓	✗
Manage Endpoints	✓	✓	✗
Generate reports	✓	✓	✓
Receive Notifications	✓	✓	✓
Endpoint Detection and Response			
Modify Policy Settings	✓	✓	✗
View Policy settings	✓	✓	✓
Suspicious Activity Remediation	✓	✓	✗
Ransomware Rollback	✓	✓	✗
Close Suspicious Activity Incidents	✓	✓	✗
View Suspicious Activity	✓	✓	✓

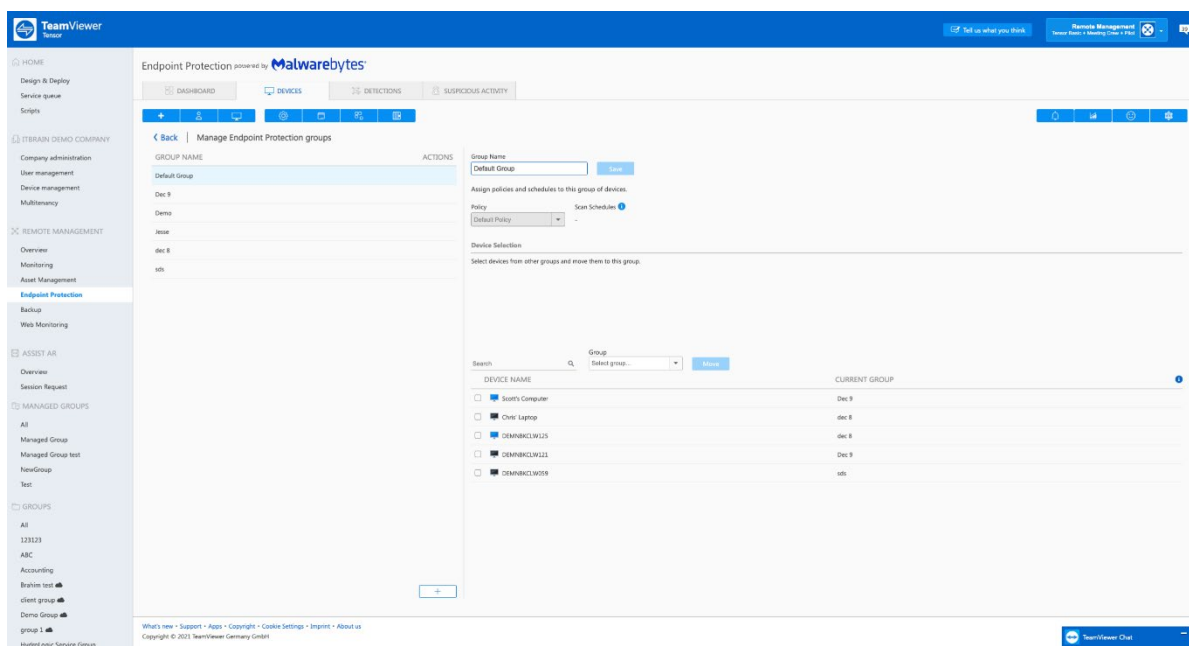
*= Applies to Assigned Groups only

5.5. Group Management

Groups are the organizational method to categorize different devices across the offices. Groups can be created, edited, assigned to different users.

The Default group cannot be deleted and all new activations will always be assigned to the Default Group.

The operations to edit and assign groups with policies, endpoints, and can be easily achieved with the settings menu.



5.6. Policies

The policy is defined as a set of settings that can be assigned to one or multiple groups and will turn on or off Malwarebytes Endpoint Protection or Endpoint Detection and Response features on the endpoint.

The Default Policy is created with a new account and it is always assigned to the Default Group. The default Policy cannot be deleted; however, it can be edited as needed.

Policies can be assigned to different groups as needed on the Groups Settings page.

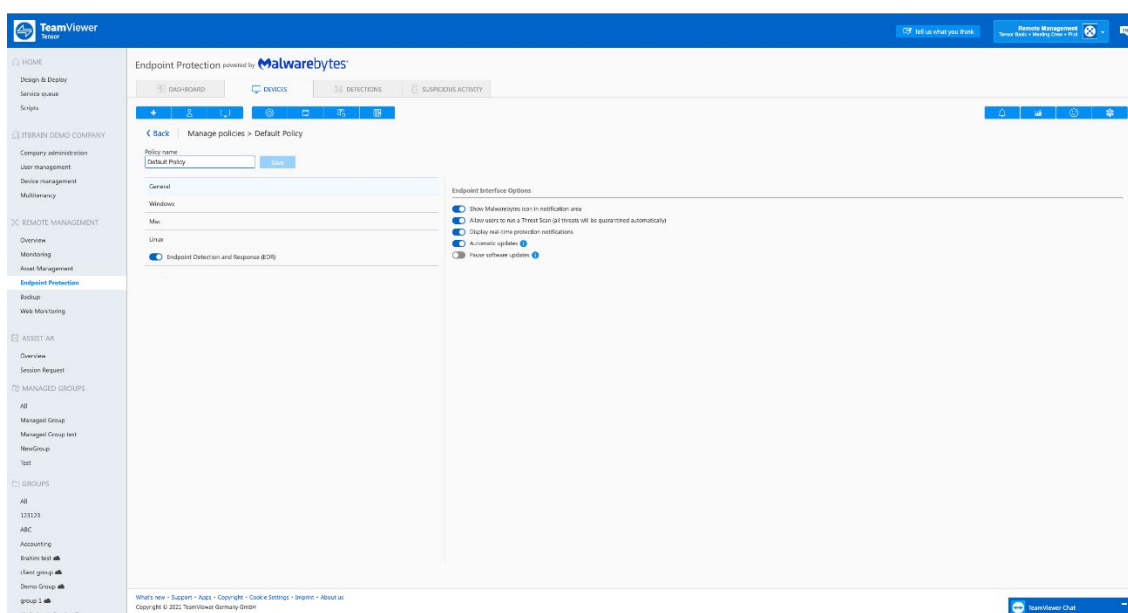
The policy is split into categories for ease of use:

5.6.1. Settings available in the TeamViewer Management Console

General

Endpoint interface Options

- **Show Malwarebytes icon in the notification area:** Shows the Malwarebytes program icon in the Windows taskbar or Mac menu bar.
- **Allow users to run a Threat Scan** (all threats will be quarantined automatically): Allows users to run Threat Scans with all detected threats put in quarantine. Users may cancel Threat Scans, but can't cancel scans controlled by the console. Threat Scans run by users are listed in the Events screen as On-demand scans.
- **Display real-time protection notifications for end-user:** Shows notifications on screen for any enabled Real-Time Protection options.
- **Automatic updates:** Automatically download and install Malwarebytes application updates (Windows only). Automatic software updates are always enabled for Mac. Malwarebytes recommends that this setting be enabled.
- **Pause software updates:** While paused, prevent Malwarebytes software from updating (Windows only). Software updates can be paused for up to 31 days. When the 31-day limit is reached, or this setting is turned off, updates will automatically resume.



Windows

Scan Options

- **Scan for rootkits on the endpoint:** A specific set of rules is used during scans to determine if a rootkit is on your device. Rootkits are malicious software that can be placed on a device and has the ability to modify operating system files and hide their presence. Toggling this setting on will make scans more intensive and effective but increase the time to complete them. By default, this setting is Off.
- **Scan the contents of compressed folders** (e.g., zip, .rar, etc.): When enabled, Malwarebytes scans two levels deep within archive zip, rar, 7z, cab and msi files. If disabled, the archive is excluded from scans. By default, this setting is On.
- **Use signature-less anomaly detection for increased protection:** By enabling this scan option, you supplement existing detection methods to use machine learning to identify malicious files.
- **Use expert system algorithms to identify malicious files:** By enabling this scan option, you supplement

existing detection methods to use expert system algorithms to identify malicious files.

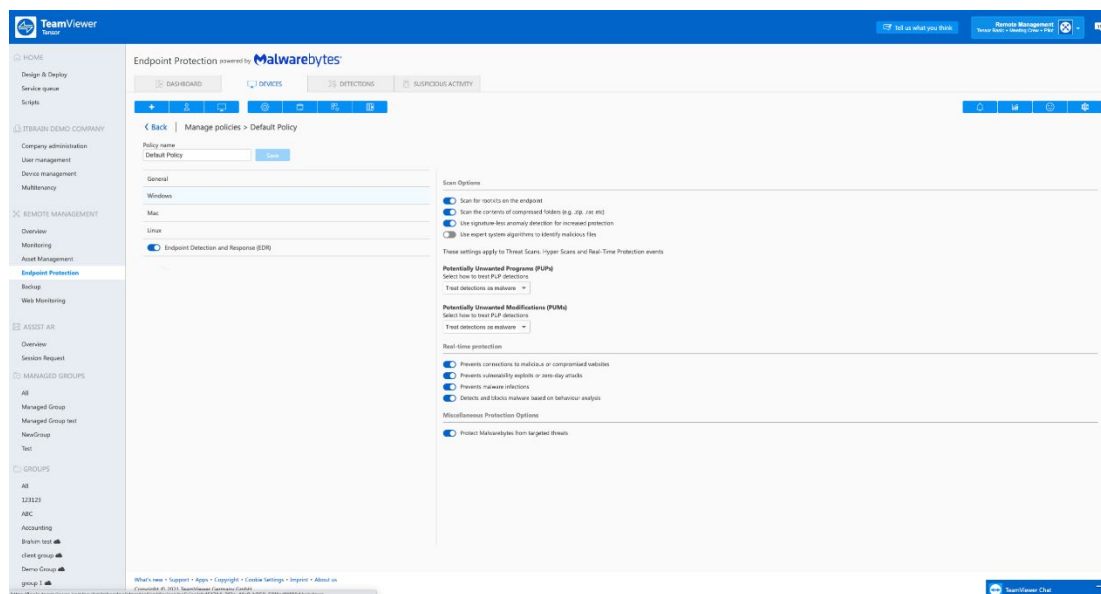
- Potentially Unwanted Programs (PUPs)
 - Treat detections as malware
 - Ignore detections
- Potentially unwanted modifications (PUMs)
 - Treat detections as malware
 - Ignore detections

Real-Time Protection

- **Prevents connections to malicious websites** (Web protection): Blocks access to and from known or suspicious Internet addresses. Disabling this feature can affect the safety of your endpoints.
- **Prevents vulnerability exploits or zero-day attacks** (Anti-exploit): Guards against vulnerability exploits for installed applications. When applications launch, Exploit Protection shields them. It can stop attacks that other security applications miss.
- **Prevents malware infections** (Malware protection): This feature protects against malicious content that tries to execute on your endpoints. Malware comes from many sources, such as downloads, external drives, and email attachments. We recommend leaving Malware Protection on. Malware Protection is always enabled on Macs using Real-time protection.
- **Detects and blocks malware based on behavior analysis**: Behavior Protection safeguards against both known and unknown ransomware. Ransomware often remains undetected until it activates. We recommend keeping Behavior Protection enabled. Behavior Protection is not supported on endpoints with Windows XP or Windows Vista.

Miscellaneous Protection Options

- Protect Malwarebytes from targeted threats (self-protection)



Mac

Scan Options

- **Scan for rootkits on the endpoint** (always enabled on macOS): A specific set of rules is used during scans to determine if a rootkit is on your device. Rootkits are malicious software that can be placed on a device and has

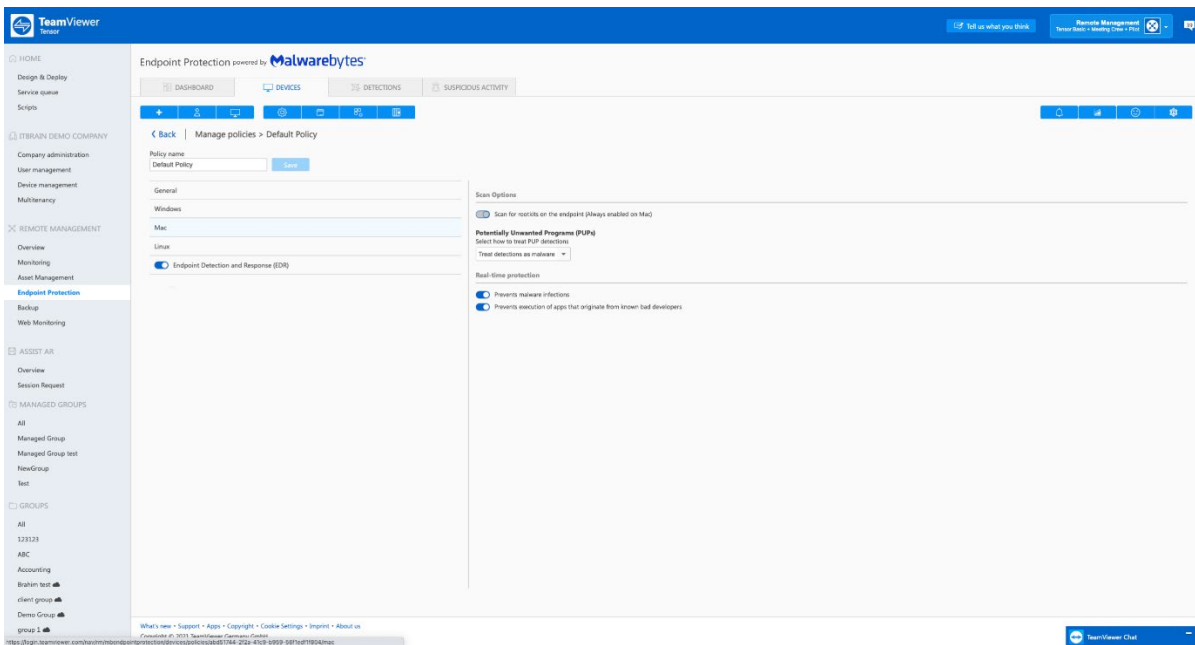
the ability to modify operating system files and hide their presence.

- Potentially Unwanted Programs (PUPs)
 - Treat detections as malware
 - Ignore detections

Automatic Software updates are automatically enabled for Mac

Real-Time Protection

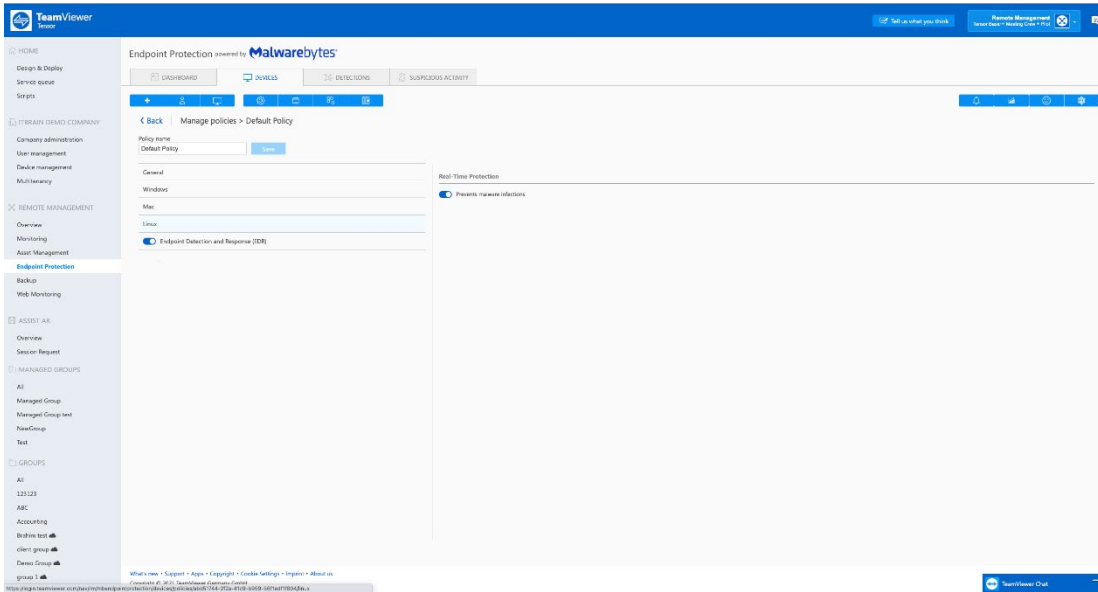
- **Prevents malware infections** (malware protection): This feature protects against malicious content that tries to execute on your endpoints. Malware comes from many sources, such as downloads, external drives, and email attachments. We recommend leaving Malware Protection on. Malware Protection is always enabled on Macs using Real-time protection.
- Prevents execution of apps that originate from known bad developers



Linux

Real-Time Protection

- Prevents malware infections (malware protection): This feature protects against malicious content that tries to execute on your endpoints. Malware comes from many sources, such as downloads, external drives, and email attachments. We recommend leaving Malware Protection on. Malware Protection is always enabled on Macs using Real-time protection.



Note: Protection updates or definition updates are configured for every hour and can be modified as needed in the Malwarebytes Nebula Console.

Note: We recommend that Real-Time Protection should be disabled when a deployment of Malwarebytes is done side-by-side with a third-party Anti-Virus solution. After deployment, only one Real-Time Protection solution should be enabled.

5.6.2. Settings available in Endpoint Detection and Response

Policy settings

Endpoint Detection and response is a policy-based product where the settings are part of the policy.

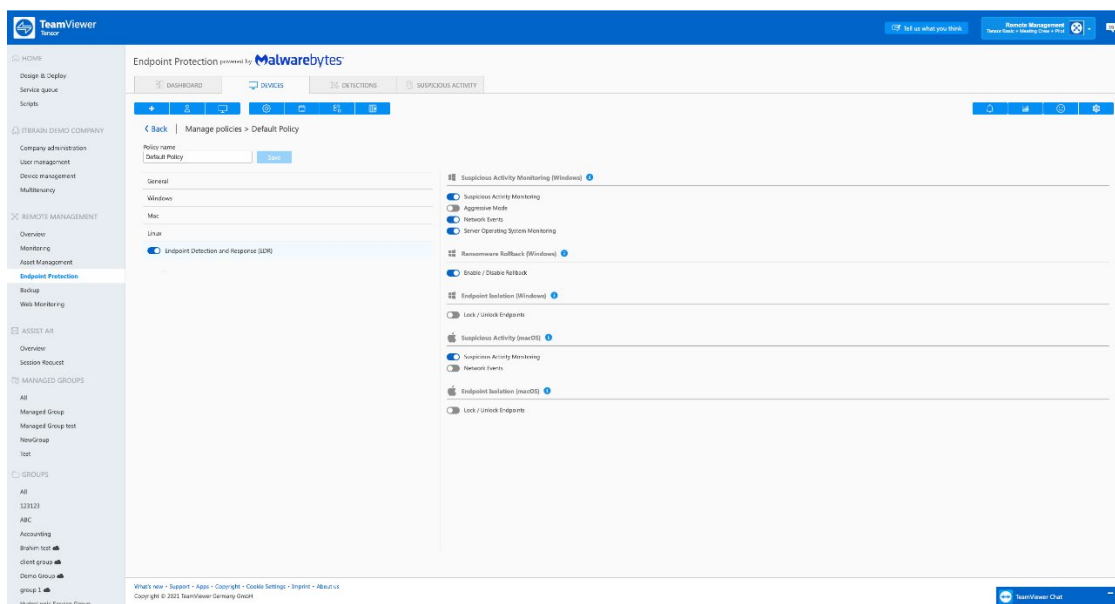
Windows

Suspicious Activity Monitoring: Enabling this in the policy will enable the Endpoint Detection and Response functionality on the endpoints and the license will be moved from Endpoint Protection to Endpoint Detection and Response. Suspicious Activity Monitoring is a feature included in Malwarebytes Endpoint Detection and Response. It watches for potentially malicious behavior by monitoring the processes, registry, file system, and network activity on the endpoint. Suspicious Activity Monitoring uses machine learning models and cloud-based analysis to detect when questionable activity occurs.

Aggressive Mode: If aggressive detection mode is enabled, Malwarebytes uses a tighter threshold for flagging processes as suspicious and is more aggressive in its detections. Aggressive detection mode helps protect your endpoints from additional unknown threats but could increase False Positives.

Network Events: The network events toggle lets you allow or restrict the collection of network events to include in Flight Recorder searches. Toggling this setting ON increases the amount of traffic sent to the cloud. By default, the toggle is set to OFF.

Server Operating System Monitoring: Enables Suspicious Activity Monitoring for server operating systems. Server OS endpoints may cause extra load with Behavioral Monitoring.



Ransomware Rollback: Ransomware Rollback is a Malwarebytes Endpoint Detection and Response feature that remediates damage done to your Windows endpoints by ransomware. Ransomware Rollback uses a special restore process to reverse the damage done by threats. Together with our Malware Removal Engine, the rollback cache allows the Endpoint Agent to restore files removed or encrypted by the malware. With rollback, a local cache is created on the endpoint to store system file changes, and this cache is used to help revert changes caused by ransomware.

Endpoint Isolation: Malwarebytes Endpoint Detection and Response includes Endpoint Isolation, which temporarily stops threats from spreading between endpoints by restricting their communication or access. An isolated endpoint can still communicate with the console and run Malwarebytes processes. Super Admins and Administrators can isolate endpoints protected by policies with the Endpoint Isolation feature enabled.

Mac

Suspicious Activity Monitoring: Enabling this in the policy will enable the Endpoint Detection and Response functionality on the endpoints and the license will be moved from Endpoint Protection to Endpoint Detection and Response. Suspicious Activity Monitoring is a feature included in Malwarebytes Endpoint Detection and Response. It watches for potentially malicious behavior by monitoring the processes, registry, file system, and network activity on the endpoint. Suspicious Activity Monitoring uses machine learning models and cloud-based analysis to detect when questionable activity occurs.

Network Events: The network events toggle lets you allow or restrict the collection of network events to include in Flight Recorder searches. Toggling this setting ON increases the amount of traffic sent to the cloud. By default, the toggle is set to OFF.

Endpoint Isolation: Malwarebytes Endpoint Detection and Response includes Endpoint Isolation, which temporarily stops threats from spreading between endpoints by restricting their communication or access. An isolated endpoint can still communicate with the console and run Malwarebytes processes. Super Admins and Administrators can isolate endpoints protected by policies with the Endpoint Isolation feature enabled.

5.6.3. Settings available in the Malwarebytes Nebula

With the Malwarebytes integration, we added the most important management settings in the TeamViewer Remote Management User Guide | 76

Management Console. A few specific settings reside in the Malwarebytes Nebula console.

For a deeper investigation or specific settings, you can log in to Nebula from the Manage Policy Menu → "Advanced settings" button located in the lower-left corner.

5.7. Scan Schedules

Malwarebytes Endpoint Protection provides multiple types of scans based on the security need on the devices.

5.7.1. Threat Scans

Threat Scans detect the most common threats by scanning conventional locations on an endpoint where threats can occur. Threat Scans use heuristic analysis, a technique that looks for certain malicious behaviors in files that Malwarebytes hasn't seen before. Run a daily Threat Scan to keep your endpoints safe.

Threat Scans check the following on your endpoints:

- **Memory Objects:** Memory allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications made during computer startup.
- **Registry Objects:** Configuration changes made to the Windows registry.
- **File System Objects:** Files that may contain malicious programs or harmful code snippets.

You may also select:

- **Quarantine found threats automatically:** It allows quarantine threats immediately when they're detected. If not selected, Malwarebytes asks you to choose an action for each threat detected.

5.7.2. Hyper Scans

A Hyper Scan is a quick scan that detects and cleans immediate threats. If a Hyper Scan finds any threats, run a Threat Scan to check for threats at a deeper level.

Hyper Scans check the following:

- **Memory Objects:** Memory allocated by operating system processes, drivers, and other applications.
- **Startup Objects:** Executable files and/or modifications made during computer startup.

You may also select:

- **Quarantine found threats automatically:** Check this box if you want Malwarebytes to quarantine detected threats without asking you. This setting may allow Malwarebytes to mistakenly quarantine programs that are not threatening, also known as a false positive detection

5.7.3. Custom Scans

Custom Scans enable you to specify what to scan. This scan is configured on the Settings > Schedules screen. When choosing a Custom Scan, the following settings are available:

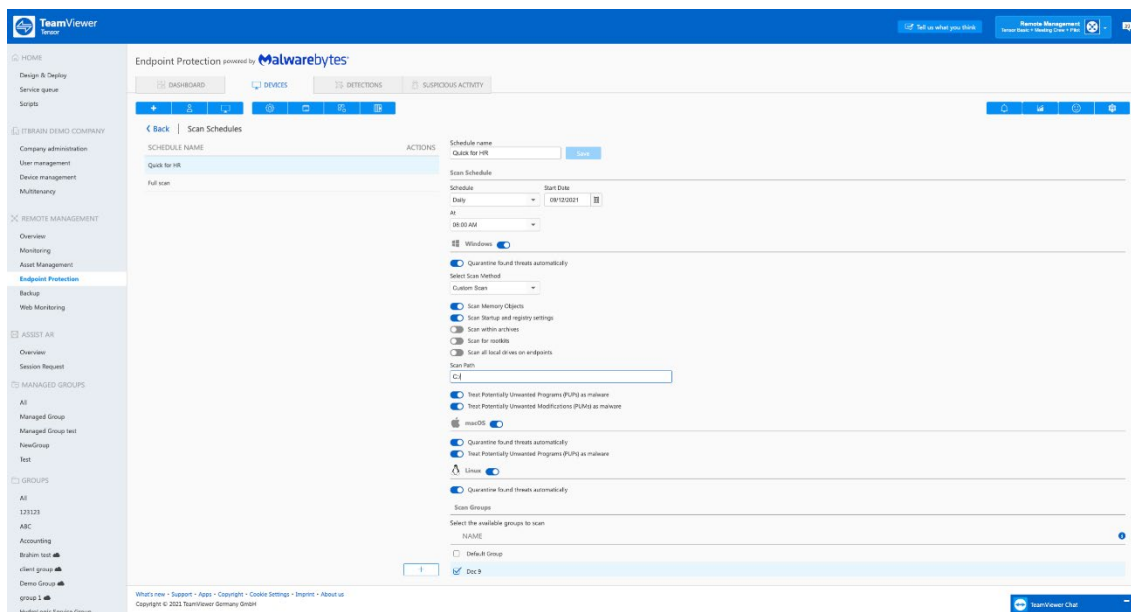
- **Quarantine found threats automatically:** Check this box if you want Malwarebytes to quarantine detected threats without asking you. This setting may allow Malwarebytes to mistakenly quarantine programs that are not threatening, also known as a false positive detection
- **Scan memory objects:** Scans memory used by operating system processes, drivers, and other applications.
- **Scan startup and registry settings:** Check this box if you want Malwarebytes to scan executable files or modifications which initiate at computer startup.
- **Scan within archives:** Archive files are scanned up to four levels deep. Encrypted archives are not scanned. Archive file types include ZIP, 7Z, RAR, CAB and MSI.
- **Scan for rootkits:** Check this box if you want Malwarebytes to look for rootkits on your device. This makes the scan take longer.
- **PUPs/PUMs:** Choose whether Potentially Unwanted Programs and Potentially Unwanted Modifications are considered malware or ignored.
- **Scan Path:** The top-level folder for the Custom Scan.

In the **TeamViewer Management Console**, you can set up scheduled scans by going from the "Device View" to the "Scheduled Scans" setting menu.

By default, for every new account, 3 scheduled scans are created and applied to the Default Group.

Multiple scheduled scans can be assigned to different groups.

Note: If a device is powered off at the scheduled time, the scan will run for the next scheduled time. In general, when the system comes online and Real-Time Protection is enabled, the system is protected even if it missed a scan.



5.8. Exclusions

By excluding specific programs, web addresses, or file locations, you can improve Malwarebytes' performance in your environment. For example, multiple security programs can interfere with each other and cause systems to slow down. You may also require exclusions if a trusted application or data file is flagged as a false positive. This article provides an overview of how exclusions work For Malwarebytes Endpoint Protection (integrated).

Only **Administrators** can create and edit exclusions as they are globally affecting the deployed fleet of devices.

You can exclude applications, files, registry keys, and IP addresses in Malwarebytes Nebula. Exclusions help prevent your Malwarebytes software from detecting and quarantining trusted items on the endpoints in your network.

By default, exclusions are applied globally to all endpoints in your network, apply exclusions to all Policies is selected by default, but you can instead select specific policies to apply exclusions. Configure your exclusions according to the needs of your network.

5.8.1.Exclusion Types

You can add several types of exclusions to meet your needs. Some exclusions support wildcards, as listed here:

- **Asterisk (*)** - Matches any number of any character.
- **Double Asterix (**)** - Matches multiple sub-folders.
- **Question mark (?)** - Matches any single character.

This table provides examples for each exclusion type:

Exclusion Type	Supported Protection Layers	Example(s)
Command Line	Suspicious Activity	test.exe /switch
Command-Line with Wildcard	Suspicious Activity	test?.bat *testscript.bat*
File by Path	Malware Protection Ransomware Protection Suspicious Activity	C:\Windows\Foo\Bar.exe
Folder by Path	Malware Protection Ransomware Protection Suspicious Activity	C:\Windows\temp\
File/Folder with Wildcard	Malware Protection	When using wildcards with folder names, a single asterisk (*) denotes any single folder, while a double asterisk (**) denotes any number of folders. C:\Users*\Documents\ C:\Users*\Desktop\test*.exe C:\temp\test?.exe C:\temp*.exe C:\Development***\Alterhostsfile.exe %PROGRAMFILES%* %PROGRAMDATA%* %PROGRAMFILES(X86)%*
File Extension	Malware Protection	ex: doc, pdf
MD5 Hash	Exploit Protection	e4d909c290d0fb1ca068ffaddf22cbd0

		9e107d9d372bb6826bd81d3542a419d6
Registry Key	Malware Protection	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fobar Note: You must use the shorthand version of the HKey entries.
Registry Key with Wildcard†	Malware Protection	HKU*\Software\Microsoft\Windows\CurrentVersion\Policies\Associations * Note: You must use the shorthand version of the HKey entries.
Web Monitoring	Website Protection	C:\Windows\Zoom\Zoom.exe
Website/IP Address	Website Protection	www.malwarebytes.com or www.teamviewer.com 234.213.143.154 2001:4860:4860::8888

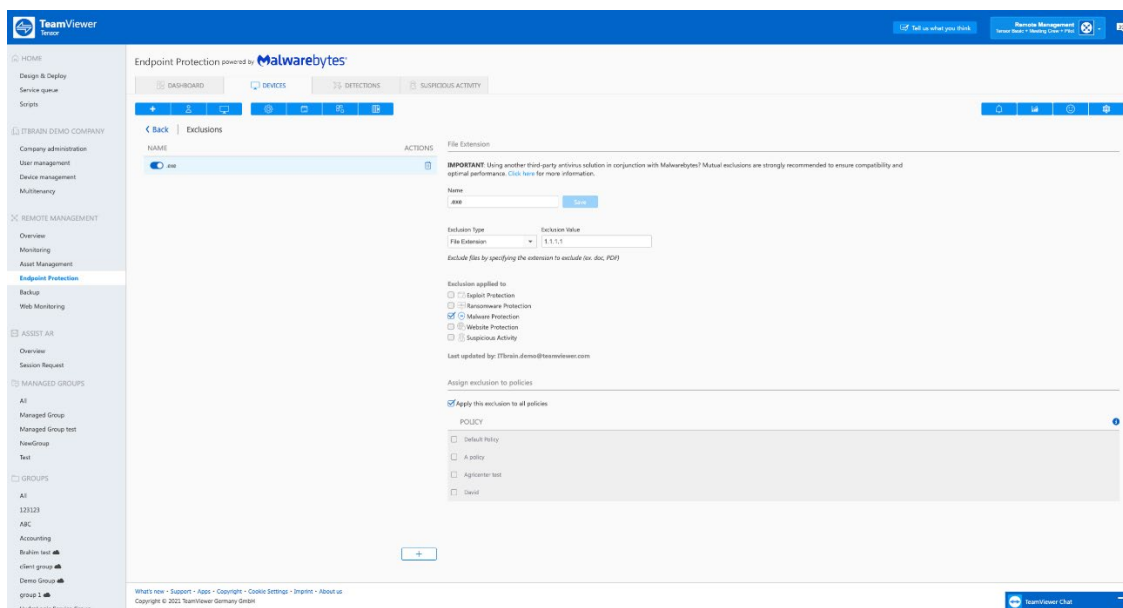
† To exclude a group of registry values using wildcards, use the format <PATH><KEY>|<VALUE>*.

5.8.2. Protection layers

When you add an exclusion, it is applied to appropriate protection layers based on the Exclusion Type. Not all exclusion types can be applied to all layers.

Use the **Exclusion Applied To** section to see on which layers the exclusions will be applied. You can deselect any layer for granular.

- **Exploit Protection:** Behavior-based detection of vulnerabilities in common programs and the operating system. Only available for Windows endpoints.
- **Malware Protection:** Real-time protection using both signature and machine learning-based detections of malicious files.
- **Ransomware Protection:** Behavior-based detection of ransomware attacks. Only available for Windows Endpoints.
 - Configure Ransomware Rollback in Malwarebytes Nebula: Configure Ransomware Rollback in Malwarebytes Nebula
- **Website Protection:** Protection from malicious network traffic, including websites or direct connections. Only available for Windows Endpoints.
- **Suspicious Activity:** Protection from anomalous files and rollback of ransomware. Only available for Windows Endpoints using Endpoint Detection and Response.



5.9. Quarantine

When malicious files are detected and quarantined, the files and registry settings are copied and encrypted into a quarantine folder on the endpoint. The Quarantine page in TeamViewer Management Console is an index for each item on the endpoint and allows you to restore or delete detected files.

While Malwarebytes Endpoint Protection engines use their best judgment whether a file is a threat or not, false positives are possible. There may be items that fall into this category but are not malicious. View detected items and cross-check the information to verify if the file is legitimate with other Threat Intelligence databases such as VirusTotal using the SHA256 hash of the file.

In the quarantine view, detections can be filtered by Group, Device, and date range.

Each Quarantine item can be expanded with a click. You can view the following information:

- **Name:** Click the name to open a glossary explanation of the detection.
- **Category:** The protection that was triggered by the detection.
- **Type:** The type of detection, such as a file or outbound connection.
- **Location:** The location of the detection on the endpoint.
- **Detection ID:** The detection identification used by Malwarebytes threat researchers.
- **Endpoint:** Click the endpoint name to go to the Overview page for the endpoint.
- **Scanned At:** Date and time when the scan occurred that found the detection.
- **Quarantined At:** Date and time when the detection was quarantined. Threats blocked by Real-Time Protection will not show the Quarantined At field.
- **Reported At:** Date and time when the quarantined detection was reported to the Nebula console.
- **Scan ID:** The identification for the scan that found the detection. Click the Scan ID to view the Scan Report for the affected endpoint.

While the **Quarantine** section shows all quarantined threats across your network, the actual threats remain in an encrypted state on the endpoints where they were found. The quarantine location is a predefined folder on your endpoints:

- **Description:** Summary of the notification.
- Click **Next**. On the **Category** page, select a notification option from the following sections:
 - **Threat activity:** All or selected threat activities and real-time protection with preferred security handling.
 - **Suspicious activity:** Notifies you of Suspicious Activity detections.
 - **Detections:** Notifies you of detection activity from Real-Time Protection, scheduled scans, and on-demand scans.
 - **User activity:** Specific conditions based on user account activity.
 - **User added:** Notifies you when a user is added to Nebula.
 - **User deleted:** Notifies you when a user is deleted from Nebula.
 - **User verified:** Notifies you when a user verifies their email.
 - **Endpoint agent activity:** Types of endpoint agent activity.
 - **Command update:** Notifies you when commands are issued to endpoints.
 - **Endpoint registered:** Notifies you when a new endpoint is registered.
- Click **Next**. Select *optional* **Conditions** if available. Click the add or delete button on the right side to add or remove a condition. (If no conditions are desired, click **Next** to skip this step.)

Field	Operator	Value	
Operating system	is equal to	Windows, Mac	+ 🗑️

- **Suspicious activity**
 - **Severity level:** Choose a severity level of All, Low, Medium, or High.
 - **Operating system:** Choose an operating system of All, Windows, Mac, Linux.
 - **Threat name:** Provide a threat name.
- **Detections**
 - **Detection type:** Choose a detection type of All, Malware, PUP, PUM, Exploit, Ransomware, Website, or Remote Intrusion.
 - **Real-time protection:** Choose to notify if True or False.
 - **Action taken:** Choose an action taken of All, Blocked, Found, Quarantined, Deleted, or Restored.
 - **Operating system:** Choose an operating system of All, Windows, Mac, Linux.
 - **Threat name:** Type a specified threat name.
- **Command update**
 - **Status:** Choose an endpoint command status of All, Created, Sent, Received, Started, Timed out, Completed, Expired, or Failed.
- Click **Next** once conditions are chosen. Select a notification delivery method of **Email** or **Webhook**.
- Enter a notification subject for the **Subject line**.
- **Choose content** based on the desired fields you want the email or Webhook notification to contain.

Select tiles to add that info to your notification

Account name
 Group name
 Machine IP
 Machine name
 OS platform
 OS release name
 Path
 Policy name
 Severity
 Status
 Threat name

6. Endpoint Protection – powered by Bitdefender (Legacy solution)

TeamViewer Endpoint Protection is our legacy endpoint protection solution which is powered by Bitdefender.

For **license activation**, please see [2.2 License Activation](#).

For **system requirements**, please see [2.3 System Requirements](#).

For **configuring policies** and assigning them to devices, please see: [3.2 Policies](#).

The configured devices are scanned and protected by the assigned policies defined under [3.2 Policies](#). Whenever malware is detected on the device, an alert is triggered and displayed as an alert message within the TeamViewer Management Console and the TeamViewer full version. An alert e-mail notification also indicates that malware was detected on one of the devices.

6.1. Activation

For activation of endpoints please see: [3.1 Activation](#)

6.2. Policies

The default Endpoint Protection policy includes the following scans and settings:

1. Quick scan, daily 09:00 AM
2. Full scan, daily at 12:00 PM
3. Real-time protection
4. Scan removable drives on connection
5. Tray icon

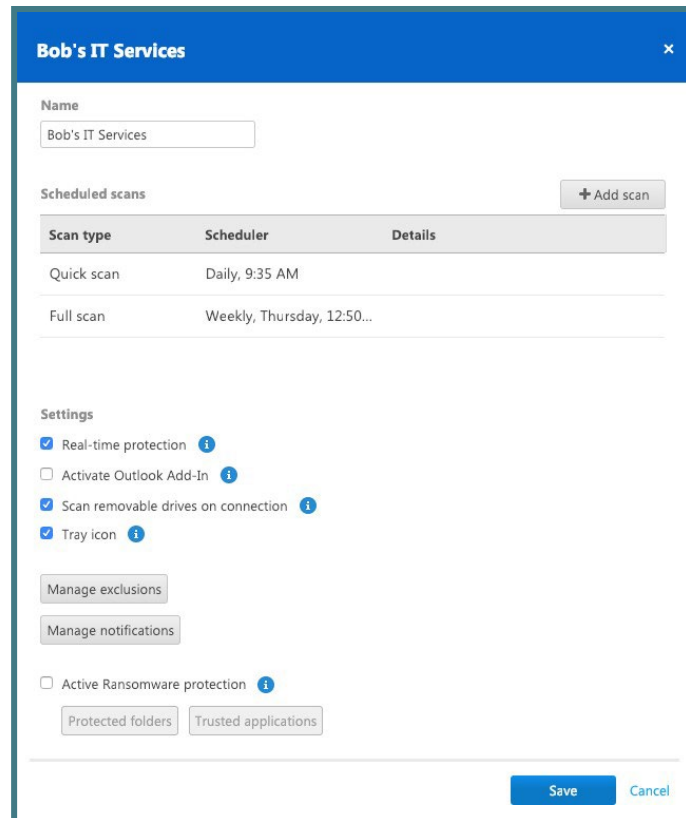


Image: Policy overview within Endpoint Protection.

6.2.1. Settings

Real-time Protection

Choose whether-or-not real-time protection should be activated for the policy. If activated, all files that are accessed (opened, running, etc.) are scanned for malware. If deactivated, threats are only detected if a scan is performed.

Note: If real-time protection is disabled, the device is potentially at risk between scans.

Outlook Add-In:

The Endpoint Protection Outlook Add-In is a Visual Studio Tool for Office Add-Ins for Microsoft Outlook. This will enable TeamViewer Endpoint Protection to delete infected attachments found in the Outlook archive files (.pst,.ost) while they are in use by Outlook.

Without this, TeamViewer Endpoint Protection is unable to delete these types of threats without first closing Outlook. The use of this feature requires the activation of the outlook add-in in the TeamViewer Management Console.

Scan Removable Drives upon Connection:

Enabling this feature automatically starts a scan on any removable drives when they are attached to the device.

Define any number of scans. Depending on the scan type and schedule, all devices are scanned for malware on a regular basis.

Click the 'Add scan' button and define a scan.

Choose between the following options:

1. **Quick scan:** TeamViewer Endpoint Protection will only scan certain data, running processes, and the registry. This way, the scan is completed quickly and the most important data is protected.
2. **Full scan:** TeamViewer Endpoint Protection will fully scan all hard drives of your devices. This scan will take longer than a quick scan. The device's data is completely protected.
3. **Custom scan:** TeamViewer Endpoint Protection will scan a defined hard drive, folder, or file. To do so, enter the path as follows: C:\Folder\Filename.fileextension

Note: Please note that the speed of your system may be affected for the duration of a scan.

Tray Icon:

This will allow the user to see the current state of Endpoint Protection, and the notifications about detected threats. The user will also be able to trigger quick and full scans.

6.2.2. Exclusions

Here, the user can specify specific drives, folders, files, or file types that should be excluded from the scan (e.g., D:\ to exclude drive D, C:\\Directory\ to exclude a folder, *.xyz to exclude a file type).

6.2.3. Notifications

The user can set up notifications via the Computer & Contact list. Endpoint protection offers the possibility to be notified for all detected threats that require immediate attention. The user can also decide if the notifications should be shown in the TeamViewer console and can also specify the e-mail address where the notifications should be sent.

If a threat is detected, Endpoint Protection will send an e-mail notification to the defined e-mail addresses. The user can enter the e-mail addresses that should receive notifications about detected threats.

You have the following options when selecting your notification settings:

4. **For all detected threats:** This is the default setting. You will be notified about any threat that is detected on one of your devices.
5. **Only when I need to take action:** If a threat is detected, Endpoint Protection moves the affected file(s) to quarantine and thus disposes of the threat. You will only be notified about a threat if you need to take immediate action (e.g. if you need to restart the computer to move a threat to quarantine).
6. **Never:** All notifications are deactivated. If you select this option, you will have to open the alert report to get information about detected threats. Even with deactivated alert notifications, your systems remain protected by Endpoint Protection.

E-mail addresses accepted by the system are the ones recognized by the TeamViewer account or company profile:

1. For TeamViewer Accounts, the e-mail address needs to be in the contact list as a contact.
2. For TeamViewer company profiles, the e-mail address needs to be a contact or a user in the company profile.

E-mail notifications are being sent from: notification@teamviewer-rm.com

Note: if working with proxy or custom firewalls, a whitelist to the domain *.teamviewer-rm.com can be added.

6.3. Dashboard

6.3.1. Manage Endpoints

This provides the user with an overview of all devices with Endpoint Protection activated. The filter on the top right of the dialog box allows users to search for a specific device by the device name. They are sorted by the device alias, where they belong to, and the policy applied to the device. Additionally, the device list can be exported as a table in a CSV file. Each device offers some important functionalities such as:

1. Devices status
2. Show threats
3. Acknowledge all threats
4. Change the policy
5. Uninstall the software

6.3.2. Manage Policies

You can select which type of scan you want and schedule the scans as follows:

6. Scan Type
 - a. Quick Scan
 - b. Full Scan
 - c. Custom Scan: this allows the user to add a specific disk, folder, or file that should be scanned.
7. Scheduler: the user can set the frequency of the scans. Users can choose between a daily, weekly, or a specific time interval (that users can set individually).

6.3.3. Manual Scans

Start a manual scan for individual endpoints. Check the endpoints for malware, regardless of scheduled scans from the Endpoint Protection policies, at any time. A manual scan will be started within the TeamViewer Management Console or the TeamViewer full version for each online device.

- In the TeamViewer Management Console, click the name of the endpoint and select 'Quick scan' or 'Fullscan.'
- In the TeamViewer full version, select the 'Quick scan' or 'Full scan' option within the context menu (right click) of the endpoint.

6.3.4. Status of the Device

For every endpoint, the status of the Endpoint Protection scan can be viewed. The status contains information about the time and date of the previous and next scheduled scans, as well as general details about the device's protection.

- Click on the name of a device and select the 'Status' option from the context menu.
- The following information is displayed in the Endpoint Protection status dialog box:
 - a. Status – the status of the device can be identified by its color.
 - i. Green: the endpoint is protected.
 - ii. Yellow: minor issue, e.g., old malware definitions or scheduled scan was not performed.
 - iii. Red: ongoing issue, e.g., malware was found but not removed.
 - b. Last Scan – date, time, and scan type of the latest scan.
 - c. Endpoint protection policy – the assigned Endpoint Protection policy.
 - d. Schedule – all scheduled scans for the endpoint as defined in the Endpoint Protection policy.

6.3.5. Quarantine

This report displays all threats in quarantine. They can be filtered by device and by a specific time interval.

6.3.6. Active Ransomware Protection

Active ransomware protection will protect specified folders to be read or written to by unknown applications such as ransomware or other malicious software. We have an intelligent system which will check read/write attempts by applications and will grant access or deny access to those folders. To use this feature, you will need to click the check box 'active ransomware protection' and set up your configurations.

Protected folders:

These are the locations the user would like to protect from being accessed or modified by untrusted applications.

Trusted applications:

These are the applications known by the user and can access or modify files within the protected folders.

Blocked applications:

This is the report of the applications which are blocked by active ransomware protection when trying to access files or folders in the user protected locations.

Note: Active ransomware protection will not be set per default. In order to use this feature, the user will need to activate it in the Endpoint Protection policy. Then, the user must make sure that at least one folder is set in the protected folders.

6.3.7. Device View

The device view of TeamViewer Endpoint Protection is designed to improve user efficiency when using the software. It gives the user an overview of all devices with Endpoint Protection activated, allowing the user to react faster when necessary. The device view first displays the devices with alarms that require immediate attention. This view is very useful for the users who manage a large number of endpoints.

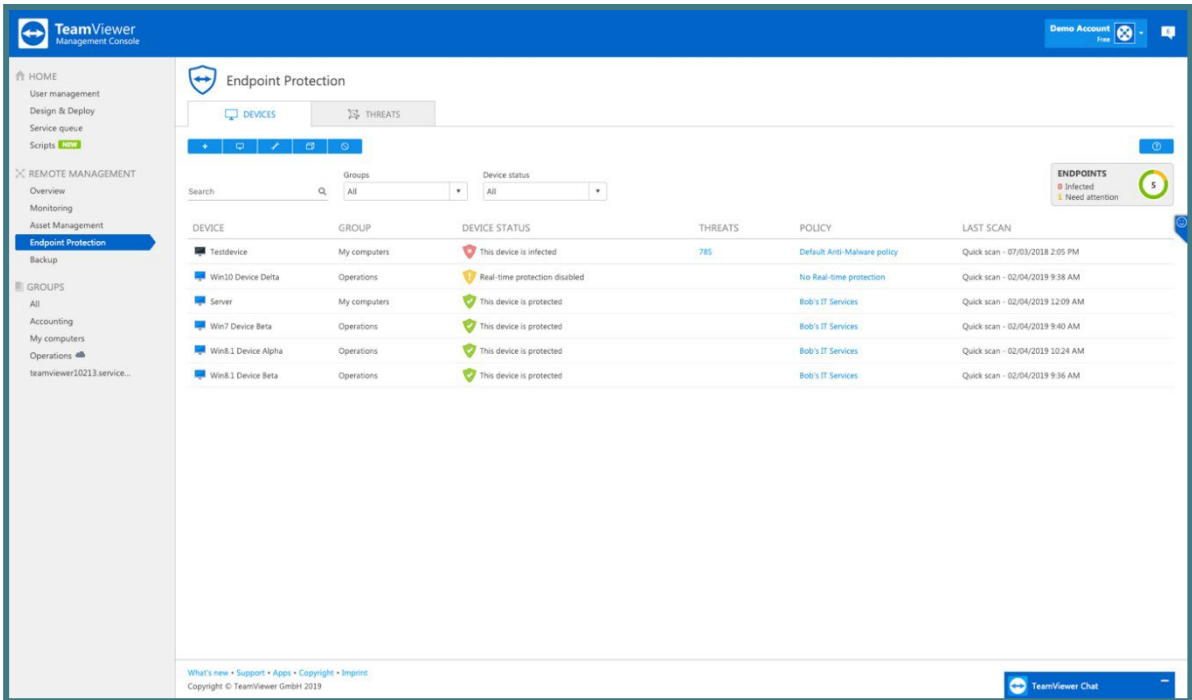


Image: Endpoint Protection device view.

Search function: This allows users to search for devices by device name. Only the endpoints with Endpoint Protection activated will be displayed.

Filtering:

By groups: Users can select only the groups with Endpoint Protection endpoints.

By device status: Users can select the devices based on their status (single and multi-selection is possible).

Endpoints: Users can see how many endpoints are available on the account, how many are in use, and how many are infected or need attention.

Devices status:

The red icon is used to identify the devices that are infected.

The yellow icon is used to identify the devices that need attention because:

1. The definitions are out of date.
2. The real-time protection is disabled.
3. No scan has been performed for a long time.
4. No policy is activated on this device.

The green icon is used to identify the devices which are safe.

By selecting the 3 dots, users can:

1. Connect directly to the endpoint.
2. Uninstall Endpoint Protection on the endpoint.
3. Trigger a quick or a full scan.

6.3.8. Threat View

The threats view shows all of the alerts for every computer that has Endpoint protection installed, and is displayed in the TeamViewer Management Console. An alert message is triggered as soon as irregularities are noticed for a device. This depends on the defined Remote Management policies.

The default Endpoint Protection policy includes the following scans, which are described in Section 5.2 Endpoint Protection Policies.

1. Quick scan, daily 09:00 AM
2. Full scan, daily at 12:00 PM

The alert report can be accessed in one of the following ways:

1. In the sidebar, click on Remote Management → select the Endpoint Protection tab → ~~at~~ the threats view tab.
2. In the sidebar, click on a group from your Computers & Contacts list → select the ~~Endpoint~~ Protection tab.

Threat details

You can display detailed information of detected malware. Quickly get information about the type of malware and be able to more effectively rate the threat of the malware.

Threat details can be accessed in one of the following ways:

1. Click the icon next to an alert message and select the 'details' option.
2. Select all of the alert messages that you wish to acknowledge, and click: Tools → ~~Details~~

The following information is displayed within the Threat details dialog box:

1. Device – name of the device where the malware was found.
2. Name – name of the malware.
3. Found in – path or file where the malware was detected.




Options: Select how you would like to proceed with the malware:

1. Delete from quarantine – select this if you want to remove the malware from quarantine and permanently delete it.
2. Restore from quarantine – select this if you want to restore the malware to its original location and remove it from quarantine.

Filtering

You can filter alert messages by Alert Type, Device, Status, and Date Range. If you click on an entry within the table header, you can sort the alert messages within the column. Using the view menu, you can define which columns should be displayed in the table and activate or deactivate the charts.

1. If a threat is detected during a scan, the detected malware will be moved to the quarantine folder immediately. The malware cannot cause any damage there. In addition, an e-mail notification is sent to the e-mail addresses you have defined for the policy.
2. The status of the alerts is indicated by different icons.

Icon Colors	Description
Red 	Malware was found on the device. The threat could not be neutralized or moved to quarantine.
Yellow 	A threat was found on the device. The threat was neutralized and moved to quarantine.
Gray 	You have acknowledged the threat. The threat is no longer displayed.

3. Confirm threat

Threats (malware) that are detected during a scan are displayed in the alert report and can be acknowledged there. Acknowledge an alert message if you know or can verify the threat and start troubleshooting. If you confirm a threat, the threat is no longer displayed in the notifications of the device, and will be displayed with a check in the alert report.

Example: Malware was found during a scan. As an administrator of the device, you will receive a corresponding notification via e-mail. Verify the notification within the TeamViewer Management Console. Now that you know what the threat is about, you can confirm the discovery of the malware and initiate measures, if necessary, in order to avoid future discoveries.

You can acknowledge threats in one of two ways:

- a. Click the icon next to an alert message and select the 'Acknowledge' option.
- b. Select all the alert messages that you wish to acknowledge and click 'Acknowledge selected.'

Note: The threat will remain in quarantine after you have acknowledged it. At your discretion, delete the malware from the device.

Tip: It is also possible to acknowledge a threat within the Computers & Contacts list (TeamViewer full version and TeamViewer Management Console).

Export

This allows you to export a list of the threats found on all your endpoints.

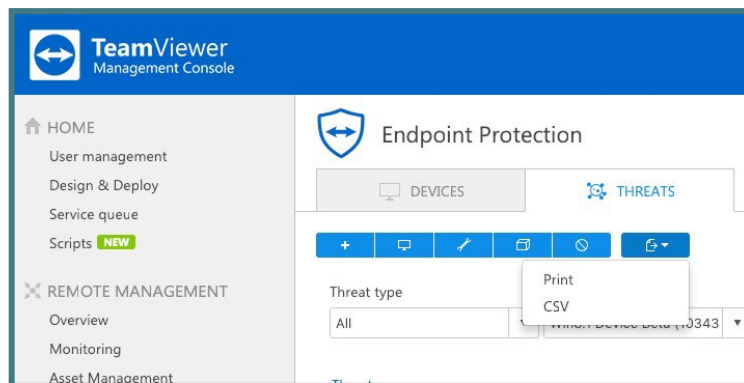


Image: Export functionality in Endpoint Protection.

Export to Print

This function will generate a web view which can be printed out or saved in any document format by using print plugins.

Export to CSV

This function will generate and download a CSV file which can be stored, managed, or modified as needed for auditability or other purposes.

7. Backup

To backup files on your devices, use the **TeamViewer Backup** service.

For **license activation**, please see [2.2 License Activation](#).

For **system requirements**, please see [2.3 System Requirements](#).

For **configuring policies** and assigning them to devices, please see: [3.2 Policies](#).

The configured devices are backed up according to the assigned policies defined under [Section 3.2 Policies](#). Whenever a backup could not be performed properly, an alert is triggered and displayed as an alert message in the TeamViewer Management Console and the TeamViewer full version.

Service icon: The user can perform the main functionalities of TeamViewer backup from the service icon. Here they can easily check the backup status on the device, start an instantaneous backup, paused a running backup or triggered a restore without a need to login to the Management Console.

The section about TeamViewer Backup will provide you with information about the version of the software currently running on the device.


Note:

1. System files are excluded from every Backup.
2. If you have selected Full backup or Quick selection, files on connected external storage drives will also be backed up.
3. As soon as a backup or restore is started, it cannot be paused or stopped.

7.1. Backup Activation

For activation of endpoints, please see: [3.1 Activation](#)

7.2. Policies

After activating TeamViewer Backup on a device, a default Backup policy which contains some basic settings is created and the user can immediately perform the first backup. The user can customize the individual backup policy, specify which data should be backed up, adjust the frequency of the backups, and even define the usage of certain process, such as the bandwidth throttling. These policies can be applied to single devices or a group of devices. In order to customize your policies, the user should navigate through the option: Manage Policy → Manage Backup policies → 

This is the starting point for policy creation and change. There are different settings which can be configured in the TeamViewer Backup policies and help the user to use efficiently the product.

7.2.1. Policy Name

The first thing to define when creating a policy is the name of the policy. Users can create many different policies, so the policy name is critical.

Next, define the name for the created policy. This name is used to identify the policy within the overview of all created policies.

The screenshot shows a configuration window titled "Default Backup policy". It contains the following elements:

- Name:** A text input field with the value "Default Backup policy".
- Selected files:** A button labeled "Full selection" and an "Edit" button.
- Backup schedule:** The text "Backup runs every 30 minutes." and an "Edit" button.
- Bandwidth throttling:** A checked checkbox, a time range slider from 8:00 to 17:00, and a "Max. bandwidth" dropdown menu set to "128 Kbps".
- Exclusions:** The text "Excluded: *.mp4; *.mp3; C:\ChristosVideos\)" and an "Edit" button.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

Image: Backup policy overview.

7.2.2. Add a Backup Policy

For more policy options please read: [3.2 Policies](#).

7.2.3. File Selection

In order to use TeamViewer Backup, the user first needs to upload data to the cloud. TeamViewer Backup offers several options to specify the data that needs to be included in the backup. This will

avoid the possibility of backing up unnecessary files, and will optimize the performance of the backup.

Backup selection

1. Full selection
 - a. This is the default backup selection. It will automatically select all files supported by TeamViewer Backup on the device.
2. Quick selection
 - a. The quick selection offers the ability to select specific file types on the device that must be included in the backup.
3. Advanced selection
 - a. With the advanced selection, the user can specify one or more specific paths that need to be backed up simply by adding the path name.

Note: When choosing 'full selection,' it is important to consider that some locations or drives are auto excluded, and the files within those locations will not be backed up.

Follow the steps below to select all files that should be included in backups using the policy.

1. Click **Edit**.
2. Select one of the following options depending on your requirements:
 - a. **Full backup:** A full backup includes all files without limitations to file type or save location on a device.
 - b. **Quick selection:** Choose the files that should be included in the backup from the most important file types. You can choose between **Office files** (documents, presentations, spreadsheets, text files, etc.), **E-mails, PDFs, eBooks, and Pictures**.
 - c. **Advanced selection:** Define a hard drive (e.g. D:\), folder (e.g. C:\Folder), a file (e.g. C:\Folder\Report.xlsx) or a file type (e.g. *.mp3) that should be included in the backup. Doing this allows users to backup specific files from individual devices.
3. Click on **Add Path**.

Note: If you select Full backup or Quick selection, files on connected external storage drives will also be backed up.

Tip: you can use placeholders to back up file paths that contain specific keywords (e.g. C:\Users\Documents).*

7.2.4.Backup Settings

TeamViewer Backup offers several options which allow for a flexible setup and ease of use.

7.2.5. Schedule Backup

TeamViewer Backup offers the ability to define the backup cycle and specify how often should the automatic backup should be performed – within a specific time interval, every day at a certain time, or specific days at a certain time.

Define when the backup for the selected files on the device should be initiated.

- To do so, click **Edit**.
- Select one of the following options depending on your requirements:
 - a. **Run backup every [X]**: Define the interval for a backup. Files will be backed up regularly regardless of date and time.
 - b. **Schedule backup for**: Define the time when the backup is performed. In addition, you can select the specific days a backup should be performed.

7.2.6. Bandwidth Throttling

With this option the user can simply limit the throughput of traffic sent to the backup servers by setting a maximum bandwidth and the timeframe for when the throttling applies.

Limit the bandwidth that is used for your backups, for example during working hours. This will reduce the effect a backup has on the speed of your internet connection.

The following settings can be configured:

- **Time frame**: Define the time when bandwidth throttling starts and when it ends. Between start and end time, the bandwidth is limited.
- **Bandwidth**: Select the maximum amount of bandwidth used during throttling.

Note: If the bandwidth is not limited, TeamViewer Backup will use the maximum bandwidth available.

7.2.7. Exclusion

TeamViewer Backup offers the ability to easily exclude specific data from the backup without impacting the whole backup selection. This can be done by specifying the path of the drives, the folders, the files, or the file types that should not be included in the backup.

Follow these steps to exclude files to the backup: click Edit → Add exclusion.

Define a drive (e.g. D:\), folder (e.g. C:\Folder), a file (e.g. C:\Folder\Report.xlsx), or file types (e.g. *.mp3) that should be excluded from the Backup.

7.2.8. Notifications

TeamViewer Backup will notify the user by sending an e-mail to the admin account in the following cases:

1. When a web restore is completed, the download link is sent in an e-mail notification.
2. When a backup failed on a device.
3. When a restore to the original device or to another device is completed.
4. When the backup storage in use reaches 75% of the purchased storage.

E-mail notifications are sent from: notification@teamviewer-rm.com

Note: If working with a proxy or custom firewalls, a whitelist to the domain *.teamviewer-rm.com can be added.

7.3. Retention Period

TeamViewer Backup offers users the ability to define how long the older version of each file should be kept in the cloud. This can be set up under the button 'Global settings' on the dashboard.

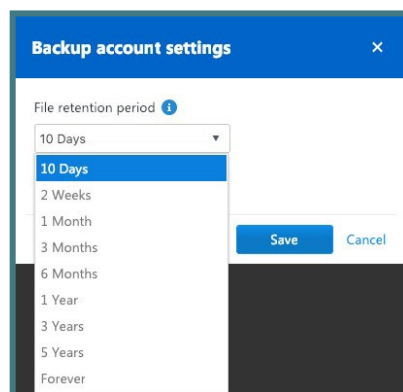


Image: Custom file retention period settings.

Note: The retention period will be applied only for the account that modified the settings and will affect all the devices with backup activated for that account.

7.4. Manage Backup

TeamViewer Backup offers flexible options to manage your backups and facilitate your work within the product.

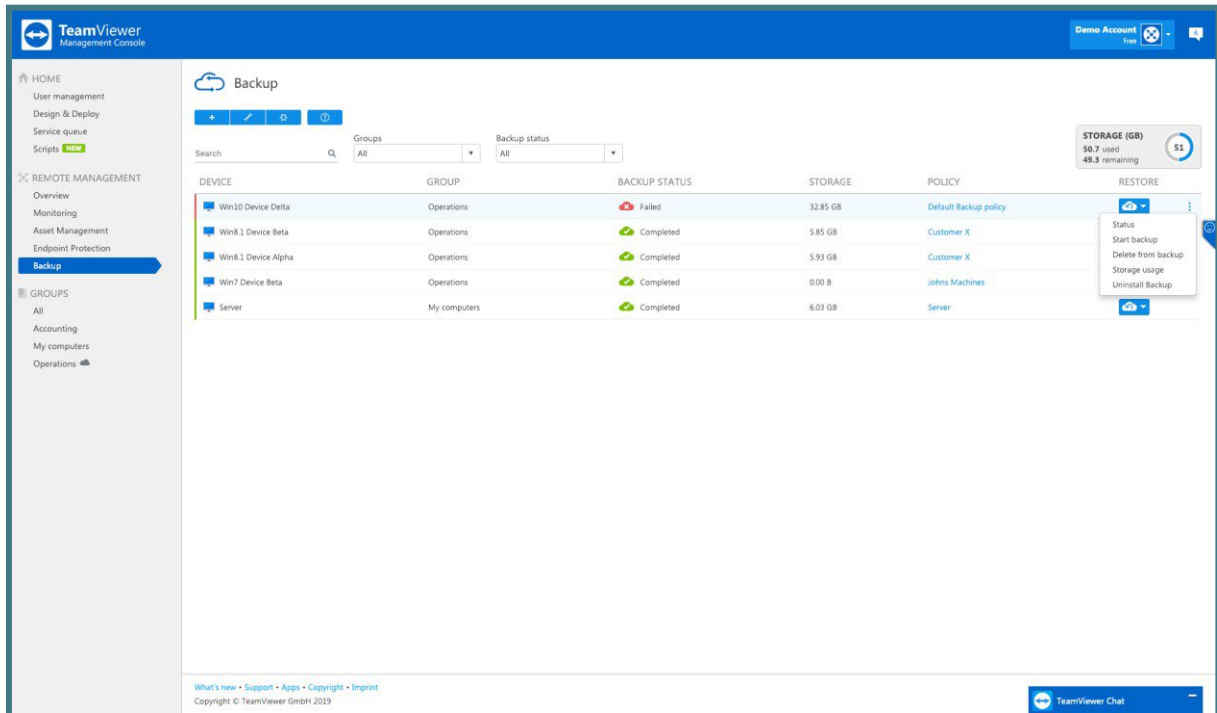


Image: Manage Backup options.

7.4.1. Backup Status

For every device, the status of its backups can be viewed in the Management Console or from the backup service icon.

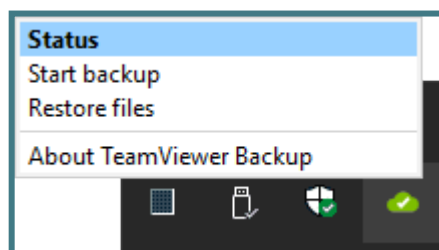


Image: Backup status view from service icon.

The status contains information about the time and date of the previous and next scheduled backup, as well as general details about the device's backup status.

1. Click on the name of a device and select 'Status' from the context menu.
2. In the TeamViewer full version, right-click on 'Status' within the context menu of the device.

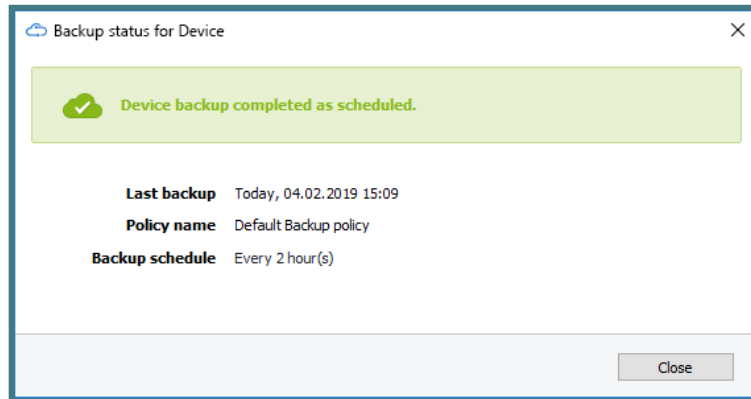







Image: Backup status service icon.

7.4.2. Status Description

The following information is displayed in the Backup status for dialog box:

1. TeamViewer Backup reports 3 different device statuses which can be identified by the following colors:

Status	Description
Green 	The backup is completed as scheduled.
Yellow 	The backup did not perform as scheduled due to a minor issue, e.g. the last scheduled backup could not be performed.
Red 	The backup failed on the device due to an ongoing issue, e.g. the latest backup failed, or several scheduled backups could not be performed.
In Progress 	The backup is being performed.
Backup paused 	The backup is paused.

2. Last backup: Date of the last successful backup.
3. Backup Policy: The assigned Backup policy.

7.4.3. Daily Storage Usage Per Device

Additionally, in order to monitor the backup storage, the user can see the how much storage space is used monthly. The user can also see how much space is used daily on each device, in a time interval of 2 weeks.

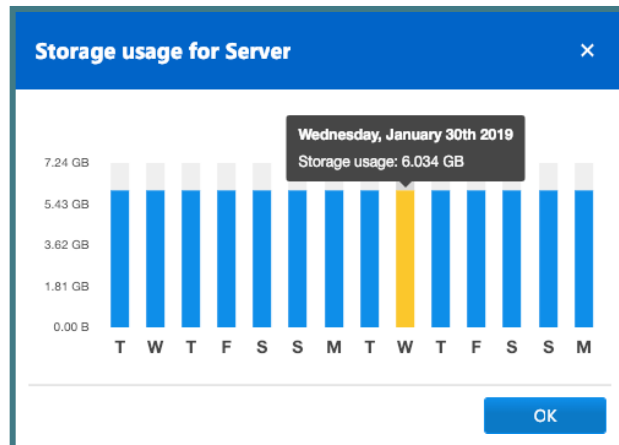


Image: Daily storage usage per device.

7.4.4. Delete Files from Backup

TeamViewer Backup offers the ability to delete unwanted files, folders, and/or drives from the backup storage. This maximizes the efficacy of the product.

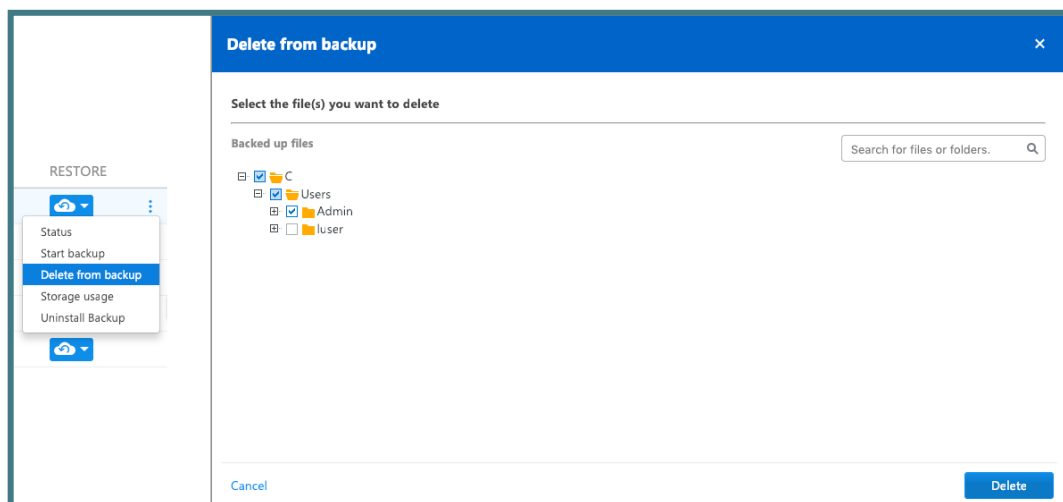


Image: Delete a file from backup storage.

7.5. Restore Backed Up Files

After a backup is successfully performed, the user can choose how the files should be restored:

1. Restore the files to the device (device alias).
2. Restore the files to another device.
3. Restore from a previous backup.

7.5.1. Restore to the Original Device

The user has the option to restore files remotely onto the device where the backup is running.

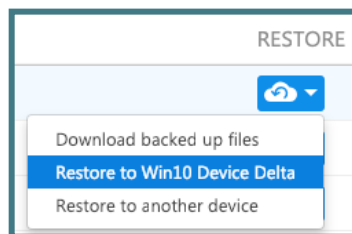


Image: Restore to the original device.

7.5.2. Restore to Another Device

The user can restore files remotely onto another device in the event that the original device is damaged or lost.

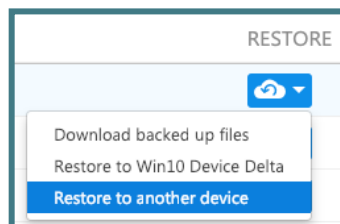


Image: Restore to another device.

7.5.3. Restore from Previous Backup

Users have the option to restore a backup that was previously performed on a prior device. This allows the user to recover older backed-up files in the event that TeamViewer Backup is re-installed on a device where a backup has already been performed.

7.6. File Selection for Restore

When selecting files for restore, the user can choose if s/he wants to 1) restore a single version of a file, or 2) restore files within a specific time interval and select the files by that particular date range. The user can also search for a file or folder by name in the search box or select the file or folder via the tree.

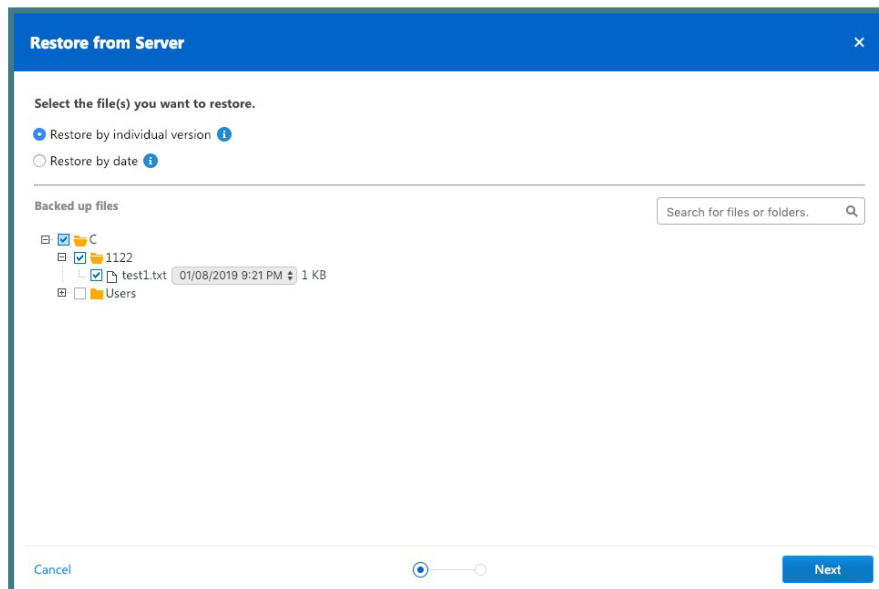


Image: Select files for restore.

After the files have been selected, the user can specify where the files should be restored to. There are two options:

1. Restore to the original location: the files will be restored to the same location they were in on the original device.

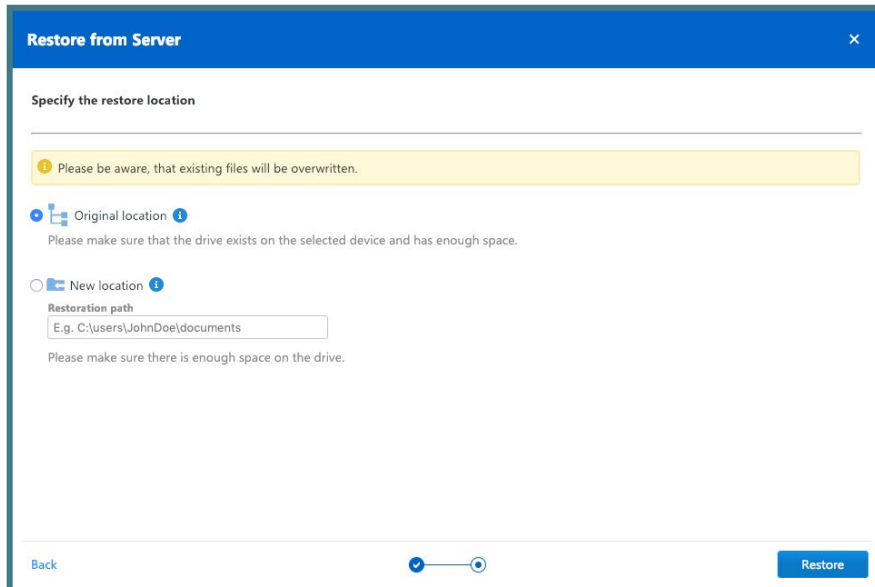


Image: Restore files to the original location.

2. Restore to a new location: a new location for the files can be chosen by adding the path of the new location.

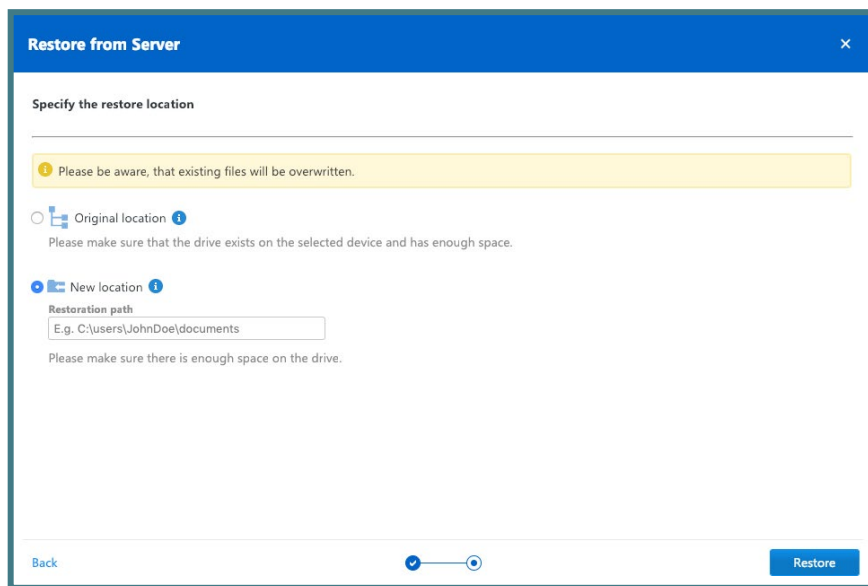


Image: Restore files to a new location.

Note: It is important to make sure that the drive(s) where the files will be restored to exists on the selected device and has enough space.

7.7. Backup Device View

The TeamViewer Backup device view is designed to make sure the user has the most important information up front. It was developed in order to make working with TeamViewer Backup easier and more efficient. By utilizing the search functions and filters, the user can search for a specific device by the device name, a group of devices, or for backup status.

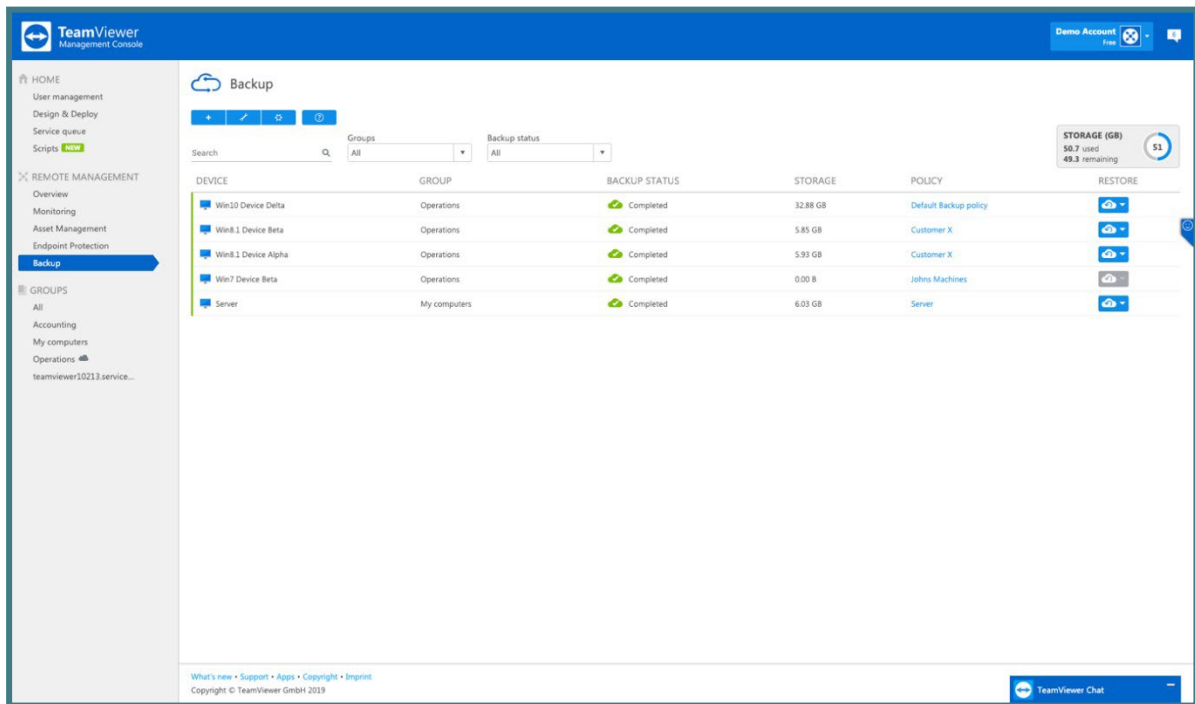


Image: Device view for Backup.

7.7.1. Filtering

The user can search for devices by the device name, or filter the devices by the groups and the backup device status.

7.7.2. Storage Used Overview

This provides an overview of the number of the endpoints in use, and displays the amount of storage used compared to the purchased storage.

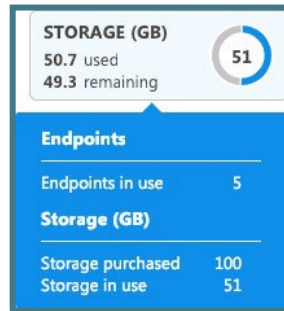


Image: Backup storage overview.

8. Web Monitoring

To monitor your web resources, use the service **TeamViewer Web Monitoring**.

For **license activation**, please see section [2.2 License Activation](#).

When all the defined conditions for a check are met, an alarm is triggered and displayed as a message in the TeamViewer Management Console . An e-mail notification will also be sent if this has been configured in the monitor configurations. An alarm message indicates that a problem has occurred on one of the monitored web resources.

8.1. Web Monitoring Activation

For activating Web Monitoring please see: [3.1 Activation](#).

8.2. Web Monitoring monitor types

There are 3 types of Web Monitors – Uptime, Page Load and Transaction.

Choose a monitor to setup

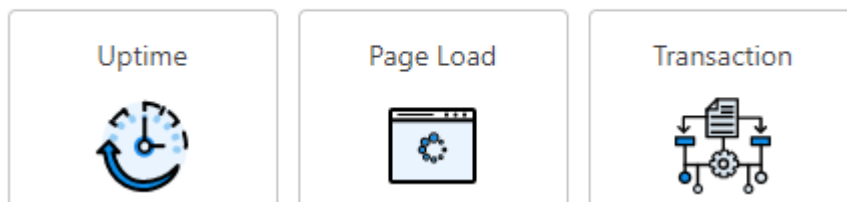


Image: Web Monitoring monitor types.

8.2.1. Uptime monitors

Checks the availability¹ and the response times of your website from multiple locations around the world. Uptime Monitoring instantly alerts you about problems with your external facing IT services. These are often the most visible to users and clients which makes them the most critical.

Uptime Monitoring can alert you of costly downtime within 1 minute of a problem by sending you email notifications.

You have the ability to create 3 sub-types of Uptime monitors - HTTP, HTTPS and ICMP (Ping).

HTTP and HTTPS – HTTP(S) monitoring allows you to test the availability and response times of your website from multiple locations around the world.

You should use HTTPS or. HTTP monitoring if your website uses HTTPS protocol for secure communication.

Once you have added a HTTP(S) monitor for your website, Web Monitoring will start sending out HTTP(S) requests to your website at your preset time intervals to check if your website is accessible.

ICMP - ICMP or Ping monitoring allows you to test the accessibility of your server over IP network from multiple locations around the world.

Once you add a PING monitor, Web Monitoring will start pinging your server at your preset time intervals to check if your URL/IP is accessible.

[Uptime monitors' advanced settings](#)

Check for String

You can use the 'check for string' or 'content matching' feature to look up a text string in the source code of your web page.

To do this, you can specify a text string under Match text in order to look it up in your website source code. If the string is not found during the monitoring check, your monitor will return a failure status. Choose between the options "Should contain" and "Should not contain" in the combo box and enter the text to match in the text box below.

For example, use "Should not contain" to make sure your web page doesn't show an error message.

¹ Availability refers to the percentage of a specified period during which a computer system can do the things it is supposed to do



Image: Check for string

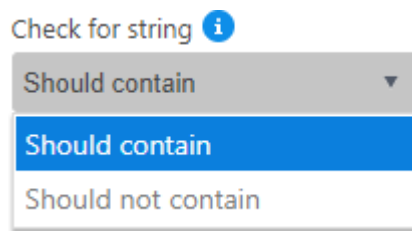


Image: Check for string combo box

8.2.2. Page Load monitors

See how long it takes to load a complete HTML page in real browsers. By tracking the load times of each individual image, CSS, JavaScript, RSS, Flash and frames/iframes, the tool measures your web visitor's user experience.

Web Monitoring's Page Load monitor is useful for understanding and analyzing things such as:

- which elements take the longest to load,
- how internal and external links are affected during loading,
- how long it takes to connect,
- the start and finish time of the load for each item on the page.

8.2.3. Transaction monitors

Transaction monitoring is proactive website monitoring that is done by deploying behavioral scripts in a web browser to simulate the path a real customer (or end-user) takes through a website.

It enables you to record interactions with a web-based application – Transaction Recorder, step-by-step and store them as a script file.

For more information on how to install the [Transaction Recorder plugin](#) and record a [Transaction Script](#) see the corresponding chapters

To precisely pinpoint the interactions, you can repeatedly playback the recording in the Transaction Recorder and edit any steps that require revision.

After the recorded script is finalized, it should be downloaded to your Local drive and then uploaded to the Web Monitoring dashboard to start configuring Transaction monitors.

When the test results become available, you can view the gathered data on the Table and Chart view dashboards: see section [7.3 Monitors data visualization](#).

8.2.4. Monitors configurations set up

Web Monitoring monitors configuration is divided into steps and is an easy process that will take you seconds to finish. To make the process easier we have added informative tooltips on the majority of the fields that will guide you to understand what each field stands for. Steps 2 and 3 are the same for all monitors types.

Uptime monitors

When configuring an Uptime monitor in Step 1 you should:

- set up a Monitor Name, provide the URL or the IP address,
- select the Protocol (http, https or icmp) based on this the corresponding monitor sub-type will be created,
- set-up the Port number, by default it is 80 for http and 443 for https,
- Select Monitor Collection, if you have any, if not, the Monitors Collection field will not be visible, to add the newly created monitor to a collection (a group). Organizing monitors in Collections is helpful when defining access to monitors in the User Management.
- select the Request method GET or POST (for POST method you should also provide the POST data the way your server expects it),
- set up the timeout threshold (in milliseconds) – the time we will wait until considering your website is down,
- set up the check frequency as often as once a minute up to once every 6 hours,

Step 2

- select from the multiple locations in Americas, Europe, Asia, Africa and Oceania where you want your website to be monitored from,

Step 3

- set up the configurations of the notifications: see section [7.4 Alarms and Notifications](#).

Monitor configuration

URL / IP i

Monitor Name

Protocol i

Request Method i

GET
POST

POST body i

Port i Timeout (ms) i

Check Frequency
 [Show advanced settings](#)

[Next](#)

Image: Uptime monitor configuration – step 1

Select the location from which you want to monitor your web resource

Locations used 2/3 i

Americas

- USA (New York City)
- USA (Los Angeles)
- Brazil (Sao Paulo)
- Canada (Toronto)
- USA (Dallas)
- Mexico (Mexico City)
- Argentina (Buenos Aires)
- USA (Miami)
- USA (Washington DC)
- USA (Denver)

Asia

- Japan (Tokyo)
- UAE (Dubai)
- Hong Kong (Hong Kong)
- Singapore (Singapore)
- South Korea (Seoul)

Europe

- Germany (Frankfurt)
- UK (London)
- Netherlands (Amsterdam)
- Switzerland (Zurich)
- Germany (Munich)
- Spain (Madrid)
- France (Paris)
- Austria (Vienna)
- Sweden (Stockholm)
- Russia (Moscow)
- Poland (Warsaw)
- Germany (Nuremberg)
- Norway (Oslo)
- Italy (Milano)
- Denmark (Copenhagen)

Africa

[Back](#) [Next](#)

Image: Monitor configuration – step 2

Set up Notifications

Enable alerting for this monitor

Trigger an alert with every single failure

Trigger an alert if there are consecutively from at least 2 locations.

Notify this contact(s) i

Ka x

Zapier Catch a Hook

Testing 06.04.21

Testing 07.04

Zapier Catch Raw Hook

Testing Zapier 08.04

Back

● — ● — ○

Finish

Image: Monitor configuration – step 3

Page Load monitors

When configuring a Page Load monitor in Step 1 you should:

- set up a Monitor Name, provide the URL or the IP address,
- Select Monitor Collection, if you have any, otherwise the Monitors Collection field will not be visible, to add the newly created monitor to a collection (a group). Organizing monitors in Collections is helpful when defining access to monitors in User Management,
- select the Browser type – you can choose which browser to run the page load checks from. Currently, we only support Firefox and Chrome. You can change the browser selection of your monitor's settings at any time,
- select the Protocol (http, https) – https is the default option,
- set-up the Port number, by default it is 80 for http and 443 for https,
- set up the timeout threshold (in seconds) – the time we will wait until considering your website is down,
- set up the check frequency as often as 5 minutes up to once every 6 hours,

Step 2 and 3 are the same as for Uptime monitors

Monitor configuration

URL / IP ⓘ
TeamViewer.com/wmdemo/

Monitor Name
Page Load Demo

Monitor Collection (optional) ⓘ
Select a Monitor Collecti... ▼

Browser ⓘ
Chrome ▼

Protocol ⓘ
HTTPS ▼

Port ⓘ
443

Timeout (s) ⓘ
30

Check frequency
15 min ▼

Back
●
○
○
 Next

Image: Page Load monitor configuration – step 1

Transaction monitors

When configuring a Transaction monitor in Step1 you should:

- browse the Script file from your local drive to start the configuration,
- set up a Monitor Name,
- Select Monitor Collection, if you have any, otherwise the Monitors Collection field will not be visible, to add the newly created monitor to a collection (a group). Organizing monitors in Collections is helpful when defining access to monitors in User Management,
- select the Browser type – you can choose which browser to run the transaction checks from. Currently, we only support Firefox and Chrome. You can change the browser selection of your monitor's settings at any time,
- set up the check frequency as often as 5 minutes up to once every 6 hours,

Step 2 and 3 are the same as for Uptime and Page Load monitors

Monitor configuration

To start monitoring proceed with the following steps:

1. Download the Transaction Monitoring Recorder plugin and install it as an add-on/extension to your Firefox or Chrome browser.

[Download Firefox Plugin](#) [Download Chrome Plugin](#)

2. Upload Recorded Script.

Script i

[Upload](#)

Monitor Name

Monitor collection i

Browser i

Check Frequency



[Next](#)

Image: Transaction monitor configuration – step 1

8.2.5. Transaction Recorder plugin installation

To start recording scripts, you will first need to download the Transaction monitoring Recorder and install it as an add-on / extension to your Firefox browser.

- To download the Recorder, simply click the Download Firefox or Chrome Plugin button in step 1 of Adding a Transaction monitor,

Monitor configuration

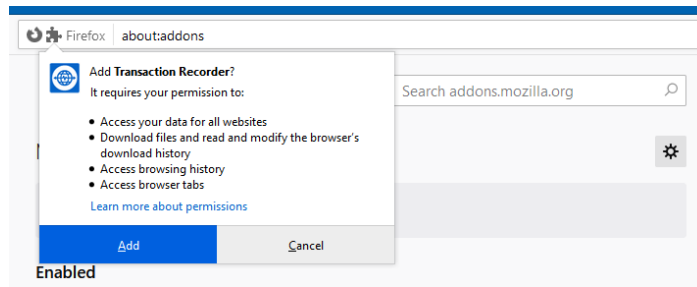
To start monitoring proceed with the following steps:

1. Download the Transaction Monitoring Recorder plugin and install it as an add-on/extension to your Firefox or Chrome browser.

[Download Firefox Plugin](#) [Download Chrome Plugin](#)

Image: Download Firefox or Chrome plugins

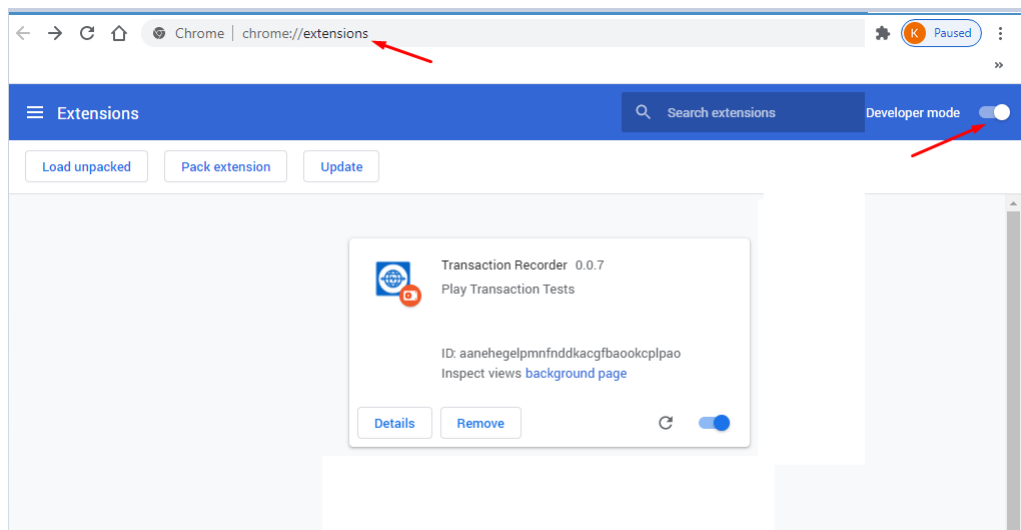
- To install the Firefox extension manually, download the XPI file, then open Firefox and select 'Add-ons' from the menu.
- Drag and drop the downloaded file into the list of currently available extensions.
- Click 'Add' button



Images: Adding Firefox extension

- To add the Recorder to Chrome, Navigate to `chrome://extensions` from your local drive.
- Activate the Developer mode (in the top right corner)
- Drag and drop the downloaded file into the list of currently available extensions.

Assuming there aren't any errors, the extension should load into your browser.



Images: Adding Chrome extension

The Transaction Recorder will now be added as an extension in your browser.

8.2.6. Transaction Scripts recording

To record a Script, open the Transaction Recorder using the icon from the task bar.

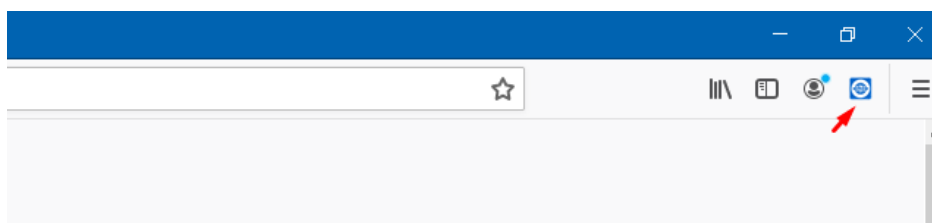
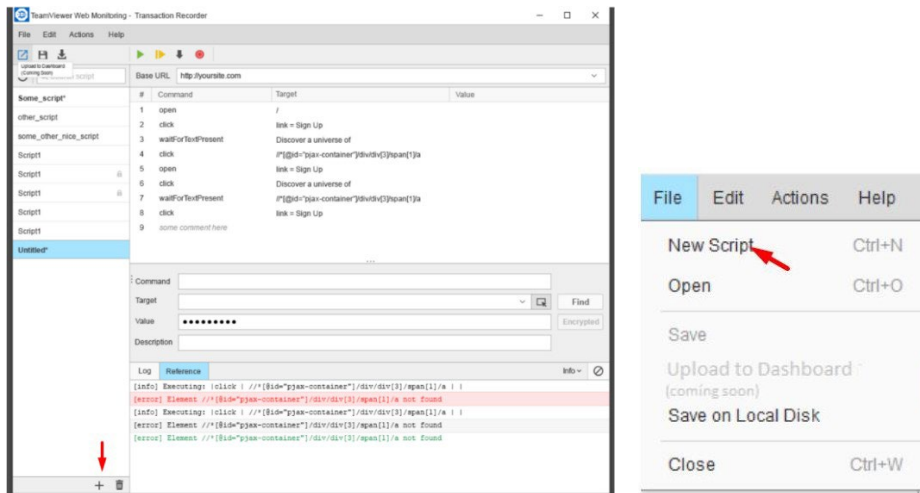


Image: Transaction Recorder icon in Firefox browser



Images: Creating new Script

1. Click the + button to start recording and adding your scripts to the bottom part or New Script in the File Menu.
2. Enter the URL of the site you want to monitor into the Base URL field (e.g. example.com) and click the Start Recording button to start recording the script.
3. Open the site that you want to monitor in Firefox or Chrome correspondingly and start navigating through and interacting with it.

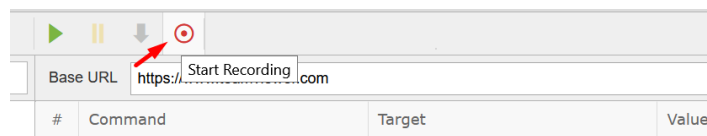


Image: Start Recording

Note: It is recommended to record the scripts in New Private (for Firefox) or Incognito (for Chrome) window. To make Transaction Recorder be also visible in Private or Incognito mode, in the Settings – Extensions - Transaction recorder – Details or Manage part activate “Allow in incognito” (Chrome) or Run in Private Windows (Firefox) setting.

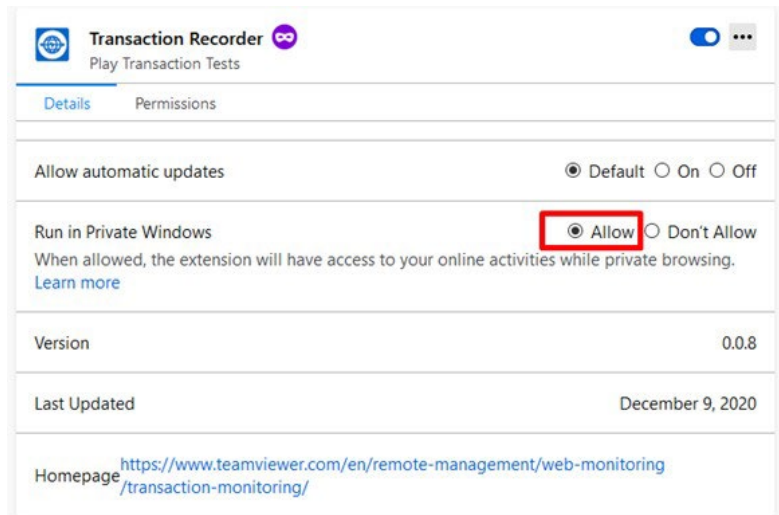


Image: Allow in Incognito or Private mode

Note: If you leave the Base URL field empty, and then press the Start Recording button and open the website that you want to record a script on, the base URL will be filled in automatically with the website's address, following the Open command added by the recorder in your script.

- The Transaction Recorder records all your steps. During the recording phase you can edit any recorded command by selecting it and editing the Command box value. You can also insert/delete commands (use the appropriate option after right clicking on a step).

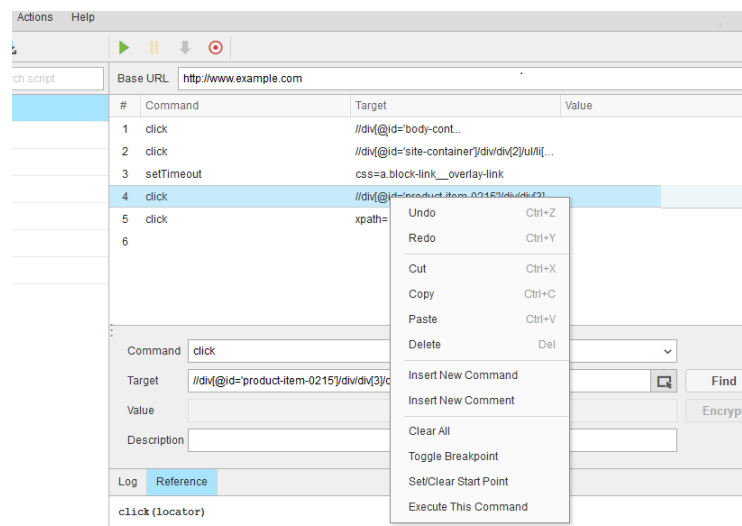


Image: Managing commands

Note: The description of the selected command is displayed in the Reference tab at the bottom of the Transaction Recorder window.

- To download the recorded script to your Local disk, click on the Download button. You can also do that from the File menu. Note that an asterisk '*' next to the script's name means that you have unsaved changes in that script.
- To edit a test previously recorded, go to the Scripts tab, choose a test from the list on the left pane of the Recorder window and click on it.

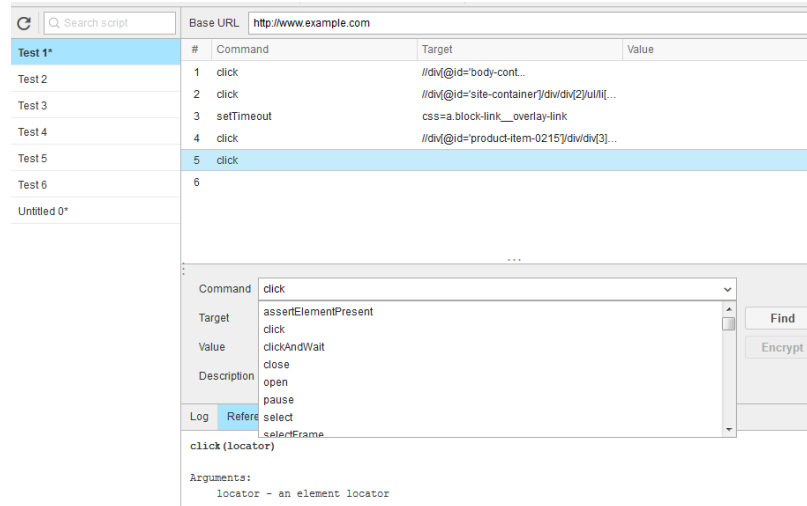


Image: Editing Script

- To save the script changes, click on the **Save** button, either in the Recorder or in the File menu. Note that the Save button remains inactive if no changes have been made in the Script.
- To view the recorded flow, click the **Run Script** button.
- You can also open/ upload other Scripts to the Recorder, to edit it or also to keep the Script on the Recorder.

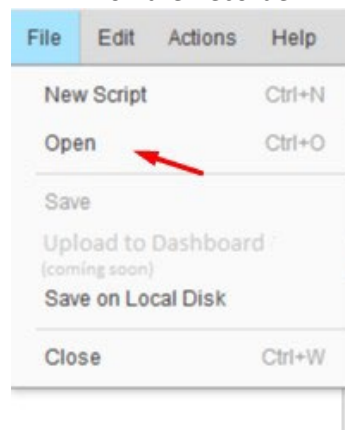


Image: Uploading script to Recorder

In the future you will also have the possibility to directly upload your scripts to the Web Monitoring dashboard and have the same Recorder plugin for a Chrome browser.

Technical hints for recording a script

- There are three fields that store essential information about each step in the script – **Command**, **Target**, and **Value**. For any element present on the web page, the Transaction Recorder maps its action with these three values: command, target, and value. For example, when typing a username in the User Name text box, the Transaction Recorder translates it as COMMAND=TYPE , TARGET=USERNAME_TEXT_BOX and VALUE=YOUR_USERNAME. For commands related to asserts, a certain value can be specified to compare to another value. For example: COMMAND=ASSERTTEXT, TARGET=LABEL and VALUE=SOMETHINGTOCOMPARE.
- The Transaction Recorder provides enough functionality in terms of identifying the target. For instance, the client can locate or identify the target using DOM, ID, Name, XPath etc. You may also find it useful to try Firefox extensions like DOM Inspector or XPath Viewer to get information about the XPath or DOM information of the GUI element under test.

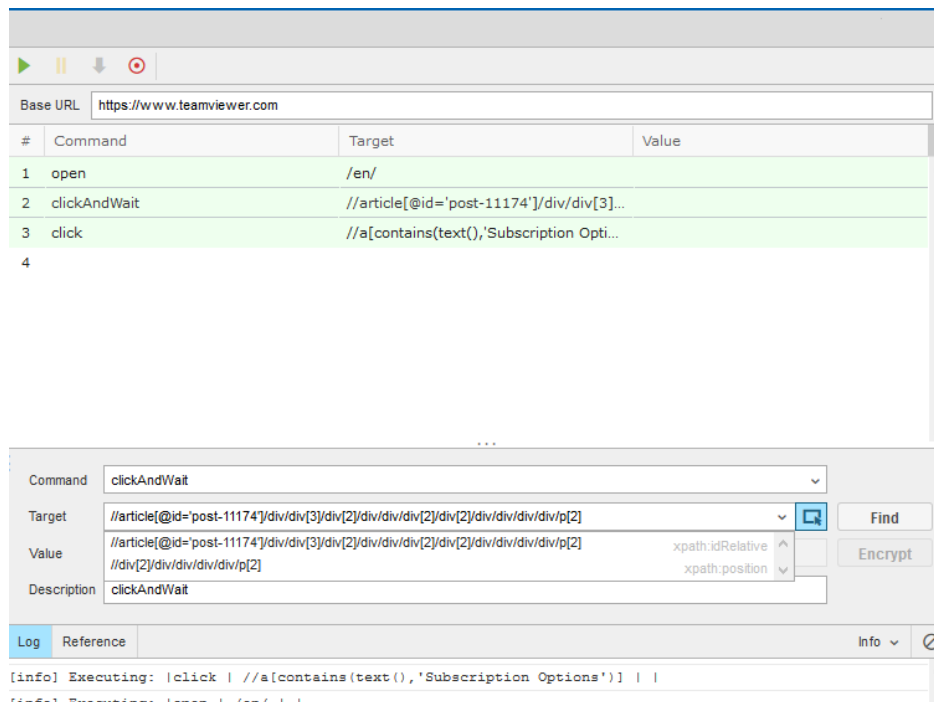


Image Identifying the target

- Use the **Target Selector** button to select the target on the web page. Click the button, and then click an element on the web page to select it. To change the selection, click some other element. To cancel the selection, click the button again.
- After you have selected the element, you can choose between ID, Name, or XPath to be the element target as needed, by selecting the value from the Target combo box.
- You can also use the **Find** button to find the element that you have specified under Target.

- There are also custom developed commands: **if**, **else** and **for**.
- If there is a need to change the flow of a transaction script by including some condition, then you can use the “**if/else**” statement. Condition of the “**if**”, “**else**” and “**for**” clauses is displayed in the Target column. When the “**else**” clause is not needed you should close the “**if**” clause using the “**endif**” command. If you are using the “**else**” command, then you should close it with the “**endElse**” command.
- In some cases, the by default added “**click**” command need to be changed to “**clickAndWait**” as it takes time to load the element or page.
- Use the “**for**” statement to repeat the same commands multiple times.

Note:

1. The default **waiting time for “Wait” commands** like open, openWindow, refresh, runScript, clickAndWait, clickHiddenElementAndWait, typeAndWait, waitForCondition, waitForElementNotPresent, waitForElementPresent, waitForNotVisible, waitForPageToLoad, waitForText, waitForTextNotPresent, waitForTitle, waitForVisible, storeEval, waitStoreElementPresent is **10 seconds**.
2. Transaction monitor has 3 min execution time limitation, it means that the **script’s runtime should not exceed overall 3 mins**.
3. Overall Script’s runtime is the sum of all pause commands time plus all potential waits on wait commands(see point 1). The Example below shows how to calculate the overall Scripts runtime
4. **Be careful using the setTimeout command** as it sets timeout for rest commands (included in point 1) in the Script, and it can make the Script’s total runtime exceed the limit of 3 minutes. Please make sure to set lower timeout for the rest commands in the Script. Default waiting value for this command is also 10 seconds.
5. The Script will fail if the provided wait time for a command is greater than it is set by setTimeout command above.

Example:

In script example below the overall Script runtime is equal to 20,000+20,000+5,000+20,000+20,000+8,000 = 93,000 ms or 93 seconds

Where

20,000 ms’s are timeout values for all “Wait” commands including open set by setTimeout command at the beginning and 5,000 and 8,000 ms are the target wait values for 2 pause commands in the Script below

```
<script>
<baseUrl>https://www.test.com</baseUrl>
<commands>
<command name='setTimeout' description='setTimeout' hideCharacters='false'>
<target>20000</target>
<value></value>
</command>
<command name='setDimension' description='setDimension' hideCharacters='false'>
<target>1920,1600</target>
<value></value>
</command>
<command name='open' description='open' hideCharacters='false'>
<target>https://www.test.com</target>
<value></value>
</command>
<command name='waitForPageToLoad' description='waitForPageToLoad' hideCharacters='false'>
```



```

<value></value>
</command>
<command name='pause' description='pause' hideCharacters='false'>
<target>5000</target>
<value></value>
</command>
<command name='waitForElementPresent' description='waitForElementPresent' hideCharacters='false'>
<target>cookieLayerAcceptButton</target>
<value></value>
</command>
<command name='clickHiddenElement' description='clickHiddenElement' hideCharacters='false'>
<target>cookieLayerAcceptButton</target>
<value></value>
</command>
<command name='waitForElementPresent' description='waitForElementPresent' hideCharacters='false'>
<target>link=Strom</target>
<value></value>
</command>
<command name='pause' description='pause' hideCharacters='false'>
<target>8000</target>
<value></value>
</command>
<command name='clickHiddenElement' description='clickHiddenElement' hideCharacters='false'>
<target>link=Strom</target>
<value></value>

```

8.2.7. Transaction recorder used commands list

N	Command name	Command Descriptions
1	click	Clicks on the element. The ".andWait" version then also waits for a page load event.
2	open	Open supports relative and full URLs.
3	type	This command erases box content, but sendkey does not
4	pause	The amount of time to sleep in millisecond. For example: "5000" means sleep for 5 seconds.
5	waitForElementPresent	Verifies that the specified element is somewhere on the page
6	setTimeout	Specifies the amount of time that the recorder will wait for actions to complete. Actions that require waiting include "open" and "waitfor" actions. The default timeout is 30 seconds.
7	clickAndWait	

8	clickHiddenElement	Clicks on a hidden link, button, checkbox or radio button. If the click action causes a new page to load (like a link usually does), call <code>waitForPageToLoad</code> .
9	storeEval	Gets the result of evaluating the specified JavaScript snippet. The snippet may have multiple lines, but only the result of the last line will be returned. Note that, by default, the snippet will run in the context of the "selenium" object itself, so this will refer to the Selenium object. Use <code>window</code> to refer to the window of your application, e.g. <code>window.document.getElementById('foo')</code>
10	select	Select an option from a drop-down using an option locator.

11	storeElementPresent	Verifies that the specified element is somewhere on the page.
12	waitForPageToLoad	Waits for a new page to load. You can use this command instead of the "AndWait" suffixes, "clickAndWait", "selectAndWait", "typeAndWait" etc.
13	if	
14	waitForVisible	Determines if the specified element is visible. An element can be rendered invisible by setting the CSS "visibility" property to "hidden", or the "display" property to "none", either for the element itself or one of its ancestors.
15	fireEvent	Explicitly simulate an event, to trigger the corresponding "onevent" handler.
16	endif	
17	selectFrame	Selects a frame within the current window. (You may invoke this command multiple times to select nested frames.)
18	selectWindow	Selects a popup window using a window locator; once a popup window has been selected, all commands go to that window. To select the main window again, use null as the target.
19	setDimension	Set the size of the current window. This will change the outer window dimension, not just the view port.
20	waitForText	Gets the text of an element. This works for any element that contains text.
21	clickHiddenElementAndWait	Clicks on a hidden link, button, checkbox or radio button. If the click action causes a new page to load (like a link usually does), call waitForPageToLoad
22	else	
23	sendKeys	Simulates keystroke events on the specified element, as though you typed the value key- by-key. This simulates a real user typing every character in the specified string; it is also bound by the limitations of a real user, like not being able to type into a invisible or read only elements
24	endElse	
25	chooseCancelOnNextConfirmation	
26	mouseOver	Simulates a user hovering a mouse over the specified element.

27	waitForElementNotPresent	Verifies that the specified element is somewhere on the page.
28	store	Returns the specified expression. This is useful because of JavaScript preprocessing. It is used to generate commands like <code>assertExpression</code> and <code>waitForExpression</code> .
29	assertElementPresent	Verifies that the specified element is somewhere on the page.
30	mouseDown	Simulates a user pressing the left mouse button (without releasing it yet) on the specified element.
31	runScript	Creates a new "script" tag in the body of the current test window and adds the specified text into the body of the command. Scripts run in this way can often be debugged more easily than scripts executed using Selenium's "getEval" command.
32	close	Simulates the user clicking the "close" button in the titlebar of a popup window or tab.
33	verifyElementPresent	Verifies that the specified element is somewhere on the page.
34	waitForCondition	Runs the specified JavaScript snippet repeatedly until it evaluates to "true". The snippet may have multiple lines, but only the result of the last line will be considered.
35	endFor	
36	for	
37	waitForNotVisible	Determines if the specified element is visible. An element can be rendered invisible by setting the CSS "visibility" property to "hidden", or the "display" property to "none", either for the element itself or one of its ancestors. This method will fail if the element is not present.
38	storeText	Gets the text of an element. This works for any element that contains text. This command uses either the <code>textContent</code> (Mozilla-like browsers) or the <code>innerText</code> (IE-like browsers) of the element, which is the rendered text shown to the user.
39	assertEval	Gets the result of evaluating the specified JavaScript snippet. The snippet may have multiple lines, but only the result of the last line will be returned.
40	mouseMove	Simulates a user hovering a mouse over the specified element.

41	echo	Prints the specified message into the third table cell in your Selenese tables. Useful for debugging.
42	assertElementNotPresent	Verifies that the specified element is somewhere on the page.
43	focus	Move the focus to the specified element; for example, if the element is an input field, move the cursor to that field.
44	storeVisible	Determines if the specified element is visible. An element can be rendered invisible by setting the CSS "visibility" property to "hidden", or the "display" property to "none", either for the element itself or one of its ancestors. This method will fail if the element is not present.
45	storeTextPresent	Verifies that the specified text pattern appears somewhere on the rendered page shown to the user.
46	addSelection	Add a selection to the set of selected options in a multi-select element using an option locator.
47	assertConfirmation	Retrieves the message of a JavaScript confirmation dialog generated during the previous action. By default, the confirm function will return true, having the same effect as manually clicking OK. This can be changed by prior execution of the chooseCancelOnNextConfirmation command.
48	verifyConfirmation	
49	createCookie	Create a new cookie whose path and domain are the same as those of the current page under test, unless you specified a path for this cookie explicitly.
50	refresh	Simulates the user clicking the "Refresh" button on their browser.
51	mouseUp	Simulates the event that occurs when the user releases the mouse button (i.e., stops holding the button down) on the specified element.
52	assertTitle	Gets the title of the current page.
53	verifyElementNotPresent	Verifies that the specified element is somewhere on the page.
54	assertExpression	Returns the specified expression. This is useful because of JavaScript preprocessing.It

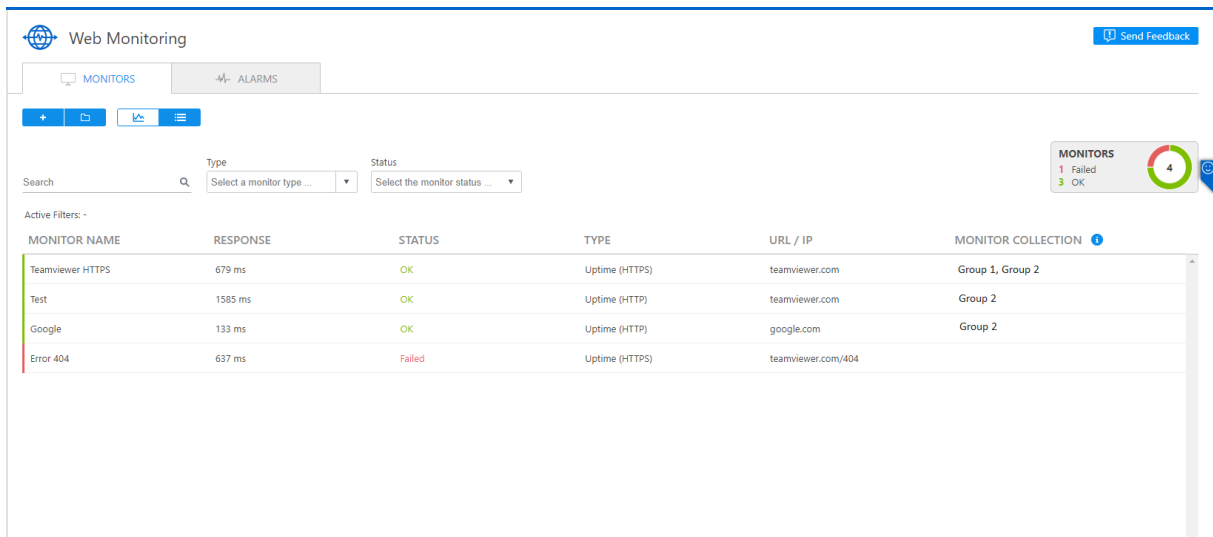
		is used to generate commands like <code>assertExpression</code> and <code>waitForExpression</code> .
55	<code>chooseOkOnNextConfirmation</code>	By default, Selenium's overridden <code>window.confirm()</code> function will return <code>true</code> , as if the user had manually clicked OK; after running this command, the next call to <code>confirm()</code> will return <code>false</code> , as if the user had clicked Cancel. Selenium will then resume using the default behavior for future confirmations, automatically returning <code>true</code> (OK) unless/until you explicitly call this command for each confirmation.
56	<code>highlight</code>	Briefly changes the <code>backgroundColor</code> of the specified element yellow. Useful for debugging.
57	<code>waitForTextNotPresent</code>	Verifies that the specified text pattern appears somewhere on the rendered page shown to the user.
58	<code>waitForTitle</code>	Gets the title of the current page.
59	<code>waitStoreElementPresent</code>	Stores if element is present on the page.
60	<code>verifyTitle</code>	Gets the title of the current page.
61	<code>check</code>	Check a toggle-button (checkbox/radio).
62	<code>typeJavaScript</code>	Sets the value of an input field, as though you typed it in. Can also be used to set the value of combo boxes, check boxes, etc. In these cases, value should be the value of the option selected, not the visible text.

8.3. Monitors data visualization

Table View

The table view is designed to display the list of monitors and the information relevant to them, such as:

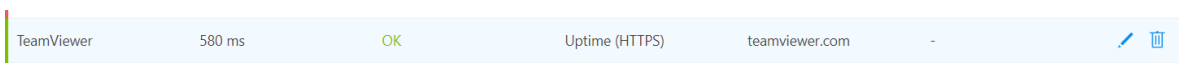
- ❓ Monitor name,
- ❓ The Response time of the last check.
- ❓ The Monitor's Status – OK or Failed, the left side of failed monitors is colored red.
- ❓ The Monitor type and the sub-types – e.g. Uptime (HTTP), Uptime (ICMP), Page Load or Transaction.
- ❓ The URL or IP – on which the monitor is running.
- ❓ Monitor Collection – the group or groups in which the monitor is part of.





MONITOR NAME	RESPONSE	STATUS	TYPE	URL / IP	MONITOR COLLECTION
Teamviewer HTTPS	679 ms	OK	Uptime (HTTPS)	teamviewer.com	Group 1, Group 2
Test	1585 ms	OK	Uptime (HTTP)	teamviewer.com	Group 2
Google	133 ms	OK	Uptime (HTTP)	google.com	Group 2
Error 404	637 ms	Failed	Uptime (HTTPS)	teamviewer.com/404	

Image: Web Monitoring table view- need to be changed

When hovering on the exact monitor row on the right corner you can see, edit and delete monitor action icons.



TeamViewer	580 ms	OK	Uptime (HTTPS)	teamviewer.com	-	 
------------	--------	----	----------------	----------------	---	---

Web Monitoring Table View, alike most of the other Remote Management products, has also the following features:

Search function: This allows users to search for monitor by name and URL or IP

Filtering: by monitor type, status and monitor collection.

By device status: Users can select the devices based on their status (single and multi-selection is possible).

Monitors Status tile

The monitor status tile is visible in both the Table and Chart view dashboard and reflects all types of monitors' status related information:

- ❓ The total number of monitors
- ❓ The number of failed and the number of OK status monitor

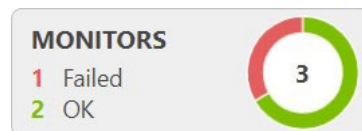


Image: Monitors status tile

Chart View

The Web Monitoring chart view shows the historical monitoring data results per check for the specified time intervals like the last hour or 3, 6, , you can also get the aggregated data time intervals, for example the last 12 and 24 hours, 3 or 7, 30 days.

The raw data for the aggregated periods is also available and can be got by clicking on the specified check point.

Soon you will be able to switch between specific dates or date ranges.

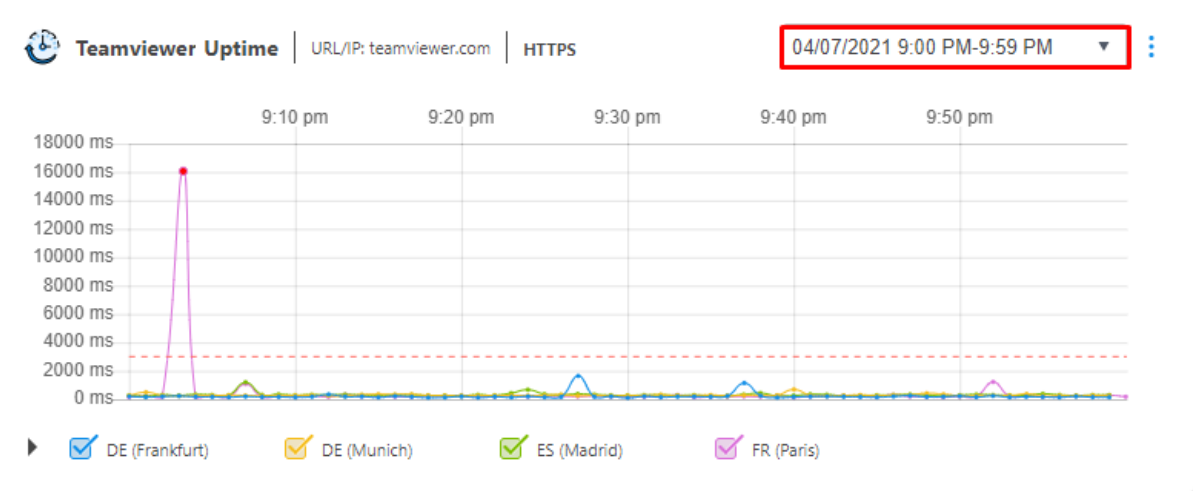
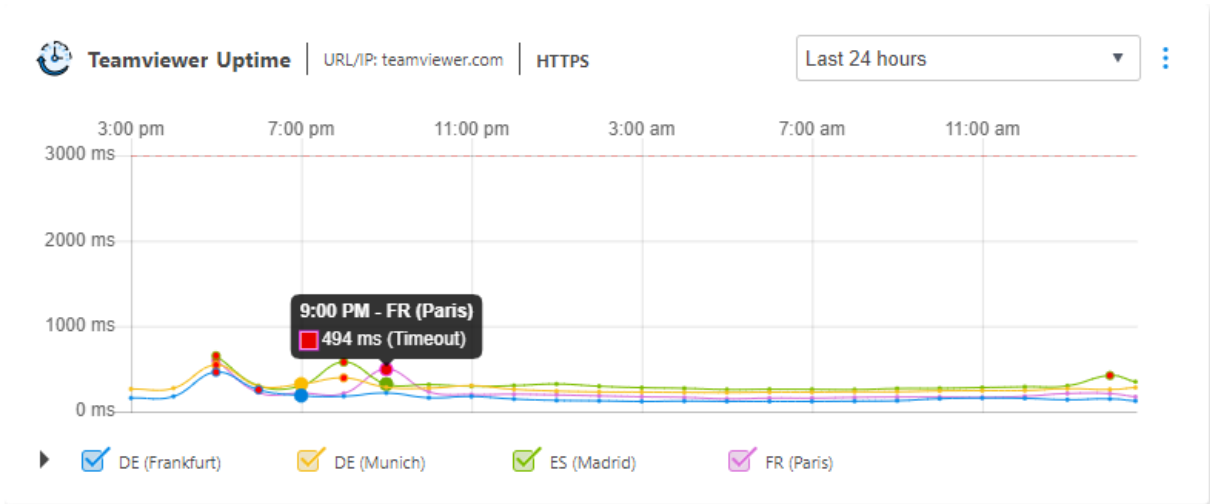


Image: Web Monitoring chart view

The top part of the Uptime monitor chart displays the Monitor name, type, URL/ IP and the uptime monitor sub-type, in the bottom part the locations from which the monitoring runs from is shown. The Page Load monitor chart's top part also shows the Browser (Firefox or Chrome) from which your monitoring runs from

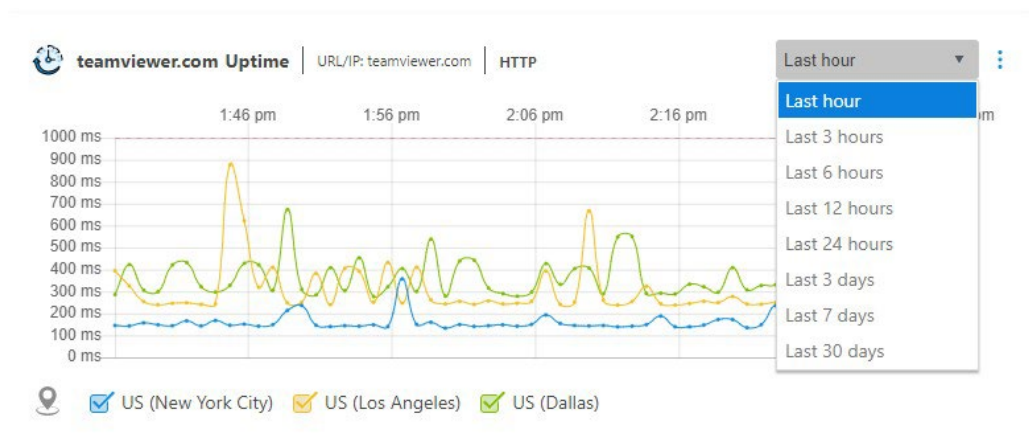


Image: Web Monitoring chart view – data ranges

The chart view clearly indicates if any check has failed. The failed checks are indicated by Red dots, when hovering on the red dot the time when the failure had occurred, the failure location ID and the failure reason are shown in the tooltip.

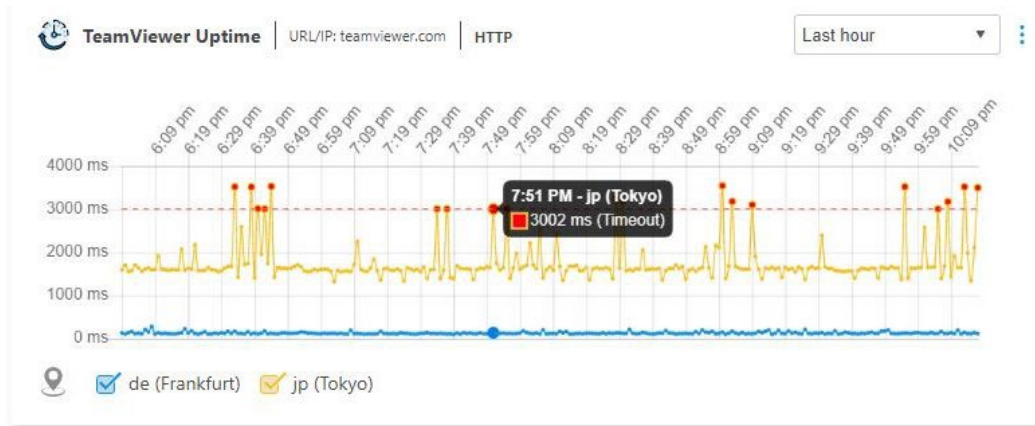
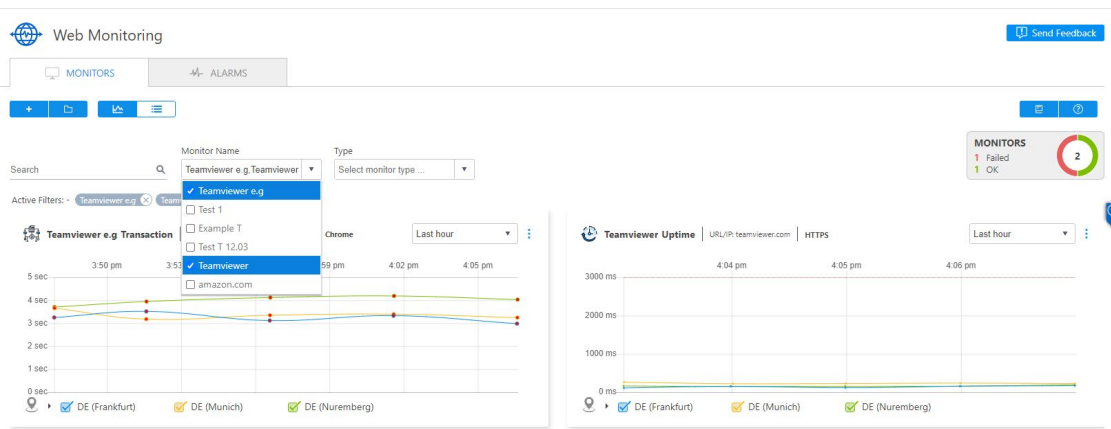


Image: Web Monitoring chart view, red dots

By using the multi selectable filters You can adjust the chart modules on the Web Monitoring dashboard the way it is suitable for you. For example, by adding the ability to put charts close together that need to be compared.

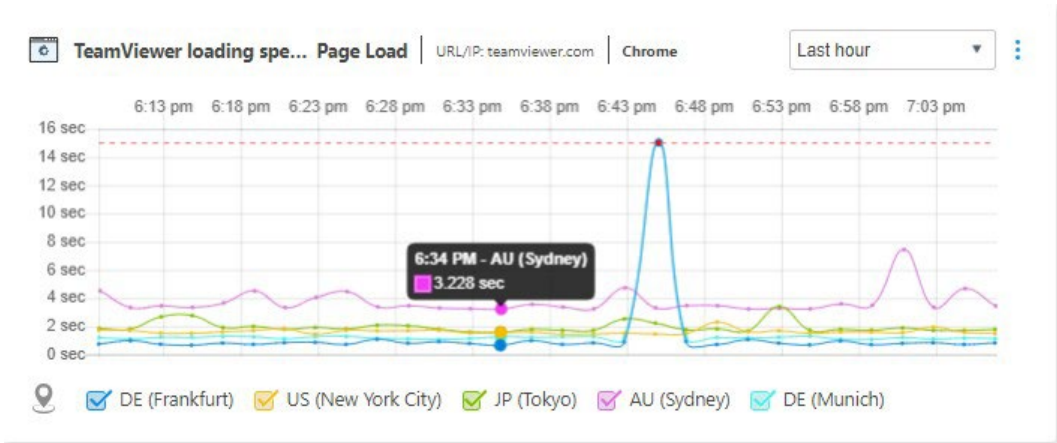


Net View – Waterfall chart and list views

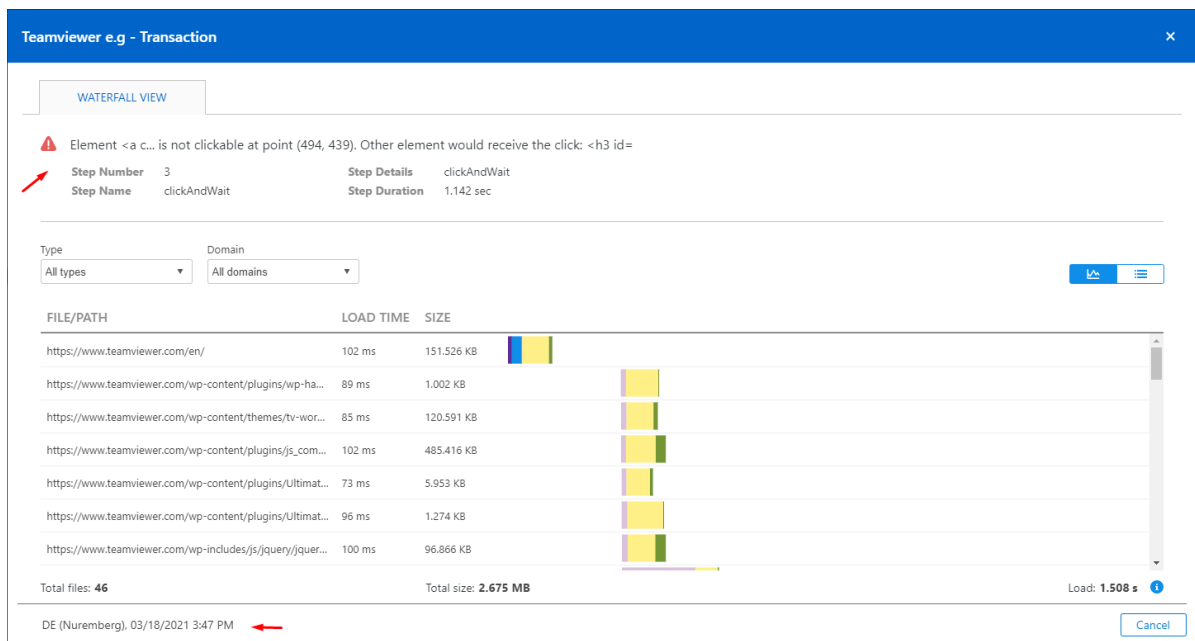
With the help of Net View you can analyze the loading times of websites in real browsers down to every single element. This allows you to see and identify where important events happened during the loading process and to find and fix issues that might be slowing a website down.

To make it more effective to use, we have also added filters for element types and domains.

To see the detailed Net View Waterfall charts and/or list views, open the Chart view and click on any Page Load monitor check point. In case of the Transaction Monitors, the Net View details are available for failed checks.

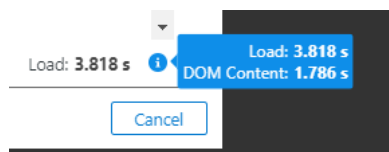


You can switch between Table and List views by clicking the respective icon on the top right corner of the Net View pop-up window.

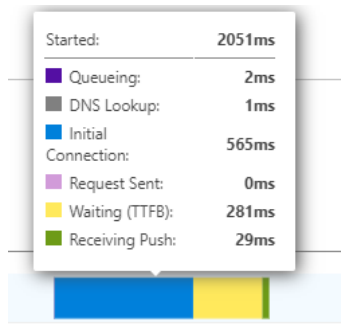


On the Chart view you can see the list of webpage elements, the size and the loading time for each one, also the total number of loaded elements, total size and overall loading time.

When hovering over the blue info icon, a tooltip with DOM Content load and Overall load time will be shown.



The Individual Elements load and starting time details like Queueing, DNS Lookup, Initial Connection, Request Sent, Waiting (TTFB) and Receiving Push are available when hovering on a specific element bar.



You can also get the Failed check information like the error message, step number, name, duration and details for Transaction monitors on the Top part of the Waterfall chart

WATERFALL VIEW

⚠ Element <a c... is not clickable at point (494, 439). Other element would receive the click: <h3 id=

↗	Step Number 3	Step Details clickAndWait	
	Step Name clickAndWait	Step Duration 1.142 sec	

Switching to Waterfall List view can be easily done by clicking on the List View button at the top right corner,

From the List view users can also Export the Net View Data to a CSV file.

TeamViewer loading speed

WATERFALL VIEW CAPTURE

Type: All types Domain: All domains Export CSV ↶ ☰

Type	STATUS CODE	TYPE	LOAD TIME	SIZE	QUEUEING	DNS LOOKUP	INITIAL CONNECTION	REQUEST SENT	WAITING (TTFB)	RECEIVING PUSH
JS	302 Redirect	Other	1140 ms	0 B	2 ms	0 ms	2 ms	0 ms	568 ms	568 ms
Image	302 Redirect	Other	96 ms	0 B	1 ms	0 ms	1 ms	0 ms	47 ms	47 ms
CSS	200 OK	Other	650 ms	0 B	625 ms	0 ms	0 ms	1 ms	21 ms	1 ms
Doc	200 OK	CSS	29 ms	0 B	0 ms	0 ms	0 ms	8 ms	20 ms	0 ms
Font	200 OK	CSS	34 ms	0 B	0 ms	0 ms	0 ms	10 ms	22 ms	1 ms
XHR	200 OK	CSS	51 ms	0 B	0 ms	0 ms	0 ms	10 ms	33 ms	7 ms
Other	200 OK	CSS	48 ms	0 B	0 ms	0 ms	0 ms	10 ms	30 ms	7 ms
https://www.teamviewer.com/w...	200 OK	CSS	43 ms	0 B	0 ms	0 ms	0 ms	10 ms	32 ms	0 ms
https://www.teamviewer.com/w...	200 OK	CSS	50 ms	0 B	0 ms	0 ms	0 ms	10 ms	39 ms	0 ms
https://www.teamviewer.com/w...	200 OK	JS	46 ms	0 B	0 ms	0 ms	0 ms	10 ms	29 ms	7 ms
https://www.teamviewer.com/w...	200 OK	JS	134 ms	0 B	0 ms	0 ms	0 ms	94 ms	38 ms	0 ms

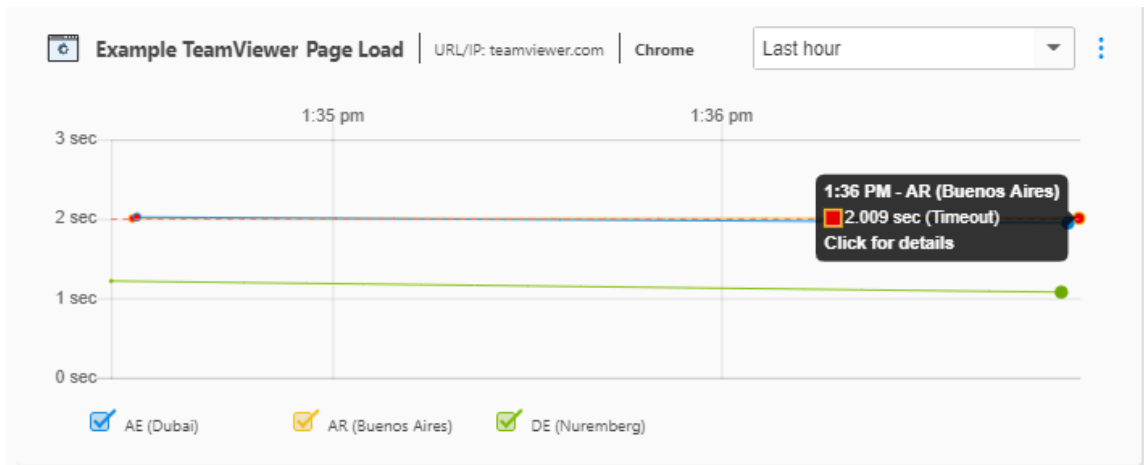
Cancel

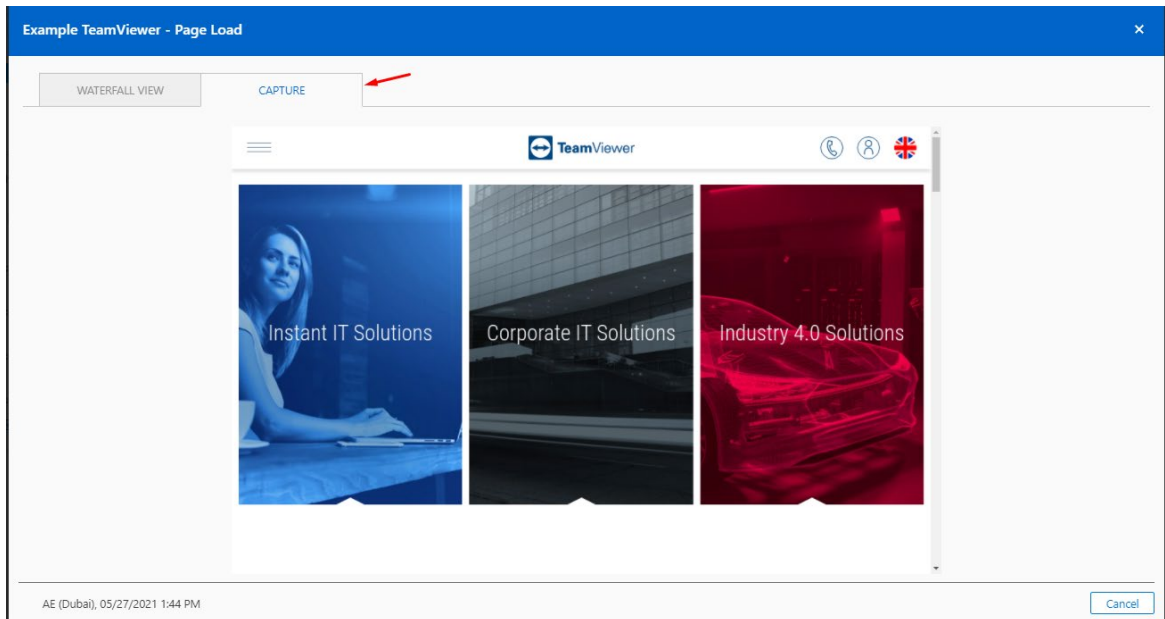
On the List View users can also see each element HTTP response Status Code which for example indicates whether a specific HTTP request has been successfully completed or was redirected.

https://www.teamviewer.com/	302 Redirect
https://www.teamviewer.com/e...	200 OK

Net View - Screen Capture

To help you to understand issues with your websites even quicker, we have added a Screen Capture functionality, which will allow them to reduce the guesswork when troubleshooting a problem. Screenshots are crucial when improving transaction errors and for analyzing page load performance. You get screenshots automatically in the Net View dialog for failed monitor checks both for Web Monitoring Page Load and Transaction monitors by clicking on the red dots in chart view graphs.

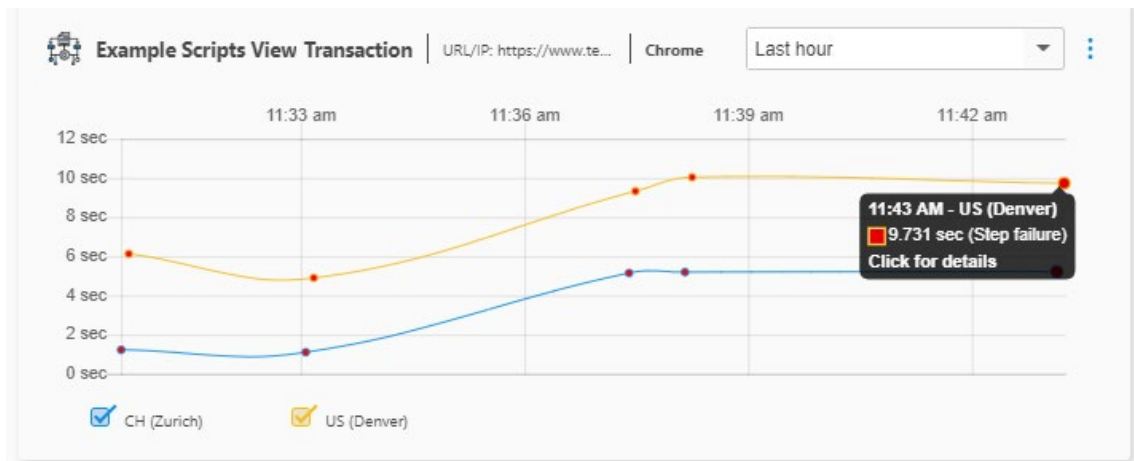


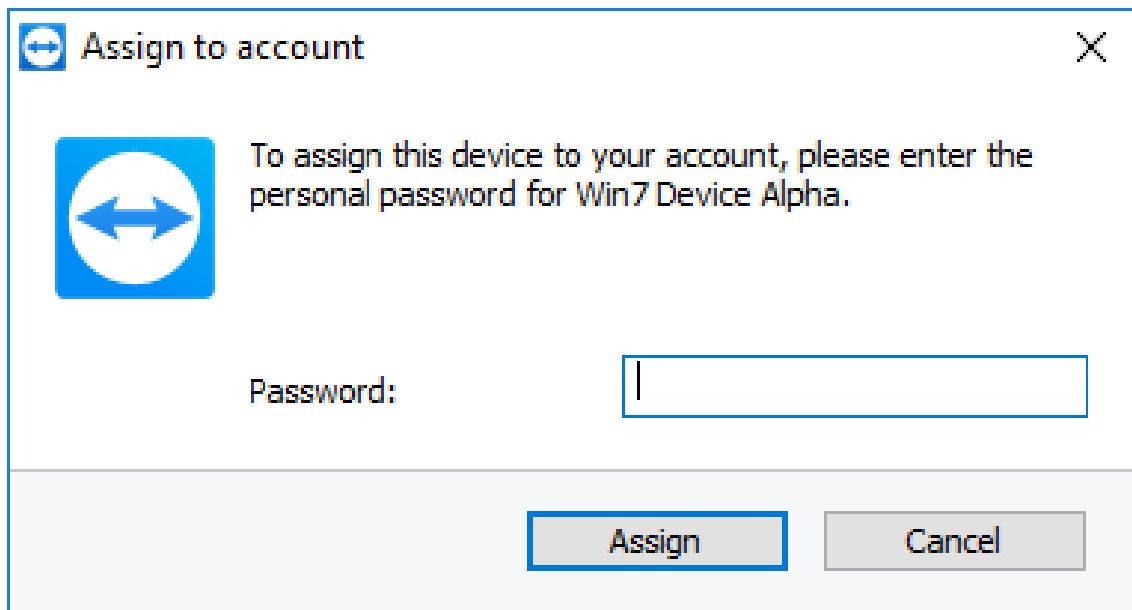


Net View - Steps View

Transaction monitors users can get the Script's steps related more detailed information to understand the duration of each step. This allows to find the weak points, analyze and improve each transaction step performance.

To get the Steps View data on Net View click on a check point in chart view graphs. Note: the step on which the script was failed are colored red and the failure details are reflected at the top part of Net View dialog





8.4. Alarms, Notifications and Error types

8.4.1. Alarms

The alarms view is focused on incident response. All raised alarms where the check threshold has been breached can be filtered, organized, and exported.

Alarms View allows you to see the severity of the alarms and take quick actions when you need to. The expandable rows allow you to see the failed check's details, like locations from where the failure comes, response time, host, error message, browser, step on which the failure occurred etc.

New alarms are added at the top of the alarms list and the left side of the row is colored red.

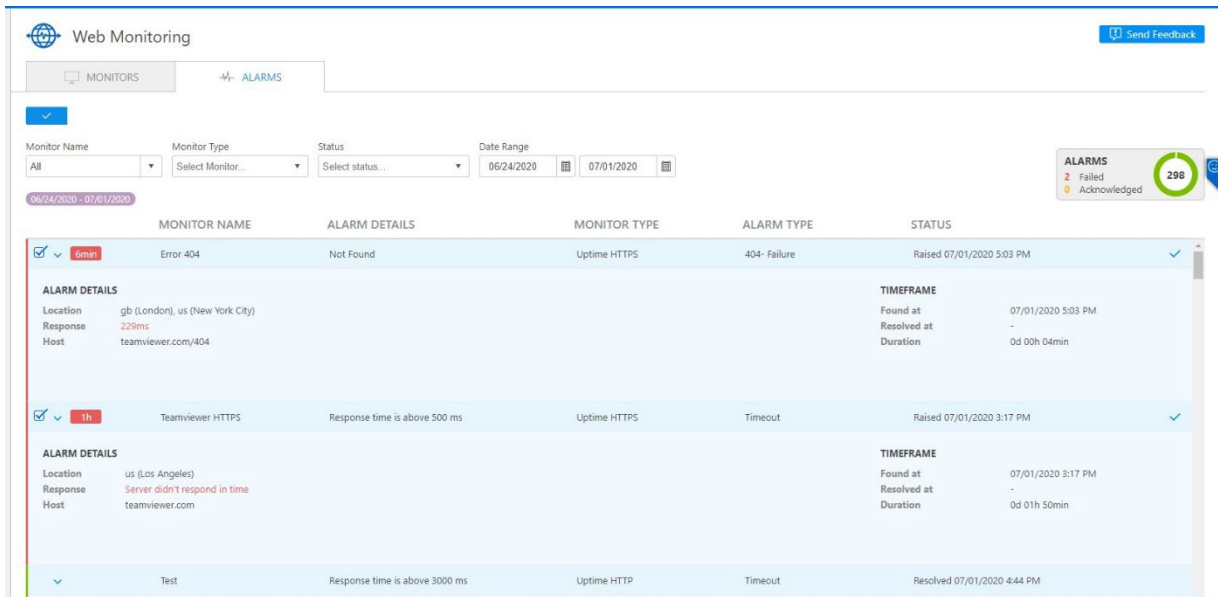


Image: Web Monitoring Alarms View

You can acknowledge the alarm by multi checking the open status alarm rows and then clicking the Acknowledge button on the left top part of the dashboard or one by one from the right part of the alarm row. When acknowledged the left part of the alarm is colored yellow.

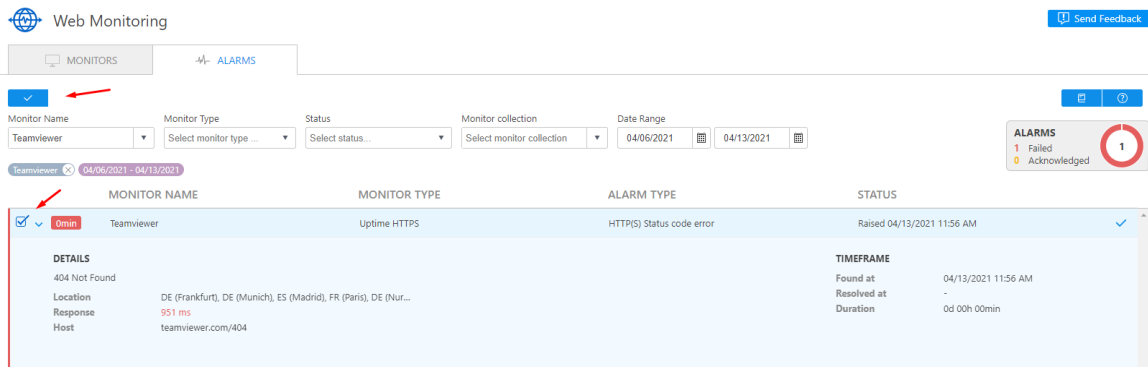


Image: Web Monitoring acknowledging alarms

Acknowledging means confirming that the alarm is noticed and actions, if needed, would be taken, so that others should not worry about this. When acknowledged the time and person who acknowledged are fixed in the Timeframe part of the Alarm.

Resolved alarms are colored green.

Like the Table and Chart views, Alarm view filtering is also possible by, Monitor name, Monitor type, Status and Date ranges.

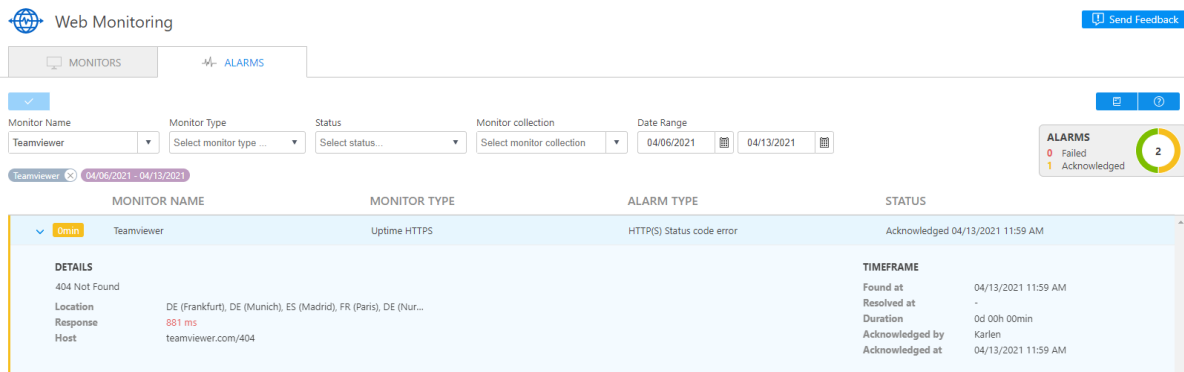


Image: Web Monitoring acknowledge details

8.4.2. Notifications

Alarm notification conditions can be set up in the monitors' configurations in Step 3 or 4 depending on the monitor type. You can be notified when E-mail addresses accepted by the system are the ones which are recognized by the TeamViewer account or company profile:

- 🔗 For TeamViewer accounts, the e-mail address needs to be in the contact list as a contact.
- 🔗 For TeamViewer company profiles, the e-mail address needs to be a contact or a user in the company profile.

E-mail notifications are sent from: notification@teamviewer-rm.com

Note: if working with proxy or custom firewalls, a whitelist to the domain *.teamviewer-rm.com can be added.

To set-up the notifications to get the emails when your monitors fail you should choose between 2 options

- 🔗 Trigger an alert with every single failure or
- 🔗 Trigger an alert if there are some (1,2 or 3) failures consecutively from any 2 locations

Set up Notifications

Enable alerting for this monitor

Trigger an alert with every single failure

Trigger an alert if there are consecutively from at least 2 locations.

Notify these Emails

Image: Set-up notification conditions

E-mail notifications regarding raised or recovered alarms and monitor types will contain the following information: Alarm Details

- 🔍 Monitor Name
- 🔍 Monitor Type
- 🔍 URL/ IP
- 🔍 Protocol
- 🔍 Request Method
- 🔍 Locations where failures come from
- 🔍 Monitors Collection
- 🔍 Transaction monitor failure description
- 🔍 Step Number
- 🔍 Step Details
- 🔍 Step Duration
- 🔍 Error Content
- 🔍 Alarm Start
- 🔍 Alarm End
- 🔍 Failure Duration

8.4.3. Error types

When your monitor fails it detects an error, based on monitor configuration it can generate an alarm. All the Alarms are available on Alarms tab – for details see the [Alarms](#) point

	MONITOR NAME	MONITOR TYPE	ALARM TYPE
<input checked="" type="checkbox"/> <input type="checkbox"/> 5d	Teamviewer	Uptime HTTPS	Timeout
DETAILS			
	Response time is above 3000 ms. Timeout while connecting to server		
Location	DE (Munich), FR (Paris), DE (Nuremberg)		
Response	6001 ms		
Host	teamviewer.com		

Image: Details section contains error related information

The following table contains the Error types and the corresponding visualization texts on Alarms tab details part and on Monitors tab, some descriptions and in some cases, the possible causes and corrective actions you may take.

Error type	Alarms Tab	Monitors tab	Notes
NetworkUnreachable HostUnreachable	Response time is above <timeout> ms or s - Timeout while connecting to server	Timeout	This timeout error can occur for Upload and FullPageLoad monitors if our server failed to connect to your website server.
ConnectionRefused ConnectionTimeout	Timeout during command execution- Timeout while connecting to server	Timeout	This timeout error can occur for Transaction monitors if our server failed to connect to your website server.
ReadWriteTimeout	Response time is above <timeout> ms or s Timeout while waiting for the response	Timeout	This timeout error can occur for Upload and FullPageLoad monitors if our server waited too long to receive a response from your website server.
	Timeout during command execution - Timeout while waiting for the response	Timeout	This timeout error can occur for Transaction monitors if our server waited too long to receive a response from your website server.
ProxyResolveError	Given proxy host could not be resolved	Proxy resolve error	This can occur if our server wasn't able to reach a remote proxy server.
HostResolveError	Given remote host could not be resolved	Host resolve error	This can occur if our server wasn't able to reach a remote host server
SendNetworkDataError	Failed to send network data	Send data error	This indicates that our server could not deliver a complete request to your website server.
ReceiveNetworkdataError	Failed to receive network data (connection reset by peer)	Receive data error	This indicates that our server failed to receive network data from your website server. Can be due to the network connection being closed while trying to retrieve a response from your website server.
TemporaryTLShandshakeError PermanentTLShandshakeError	TLS Handshake error	TLS Handshake error	This error can occur while establishing secure connections using the TLS protocol.
HttpResponseCodes	<Status code + description>	HTTP(S) Status code error	Uptime - HTTP and HTTPS example : "500 Internal Error" or " 403 Forbidden" or "404 Not found"
DnsErrorDetails	Name not resolved	DNS error	
InvalidConfigDetails	Invalid monitor	Configuration error	

	configuration		
UnsupportedBrowserDetails	Unsupported browser	Browser type error	
UnsupportedScriptTypeDetails	Unsupported script type	Script type error	
UnsupportedCommandDetails	Unsupported command in script	Command type error	
InterruptedErrorDetails	Execution has been interrupted	Execution error	
StepNotExecutedDetails	Step execution failed	Step failure	
ElementNotFoundDetails	Element was not found	Element error	
UnknownErrorDetails	Unknown error	Unknown error	
Content matching issue	Content matching failure	Matching error	

8.5. Monitor Collections and User Management

8.5.1. Monitor Collections

Allow you to group monitors in various Collections. There is no limitation to the number of monitors that can be added into a collection/ The same monitor can be attached to more than 1 collection.

To add a Monitor Collection, you should click the folder icon in the top left part of the Table or Chart View dashboards.

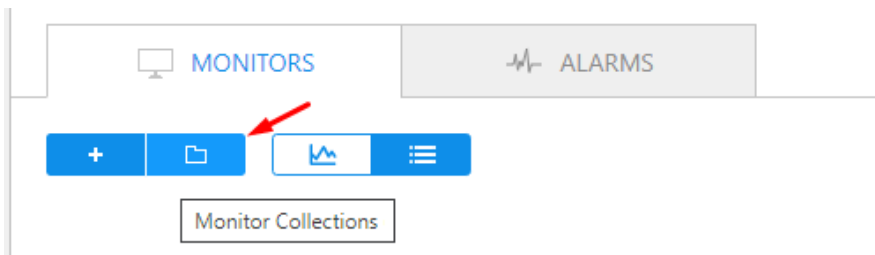


Image: Adding monitor collection 1

On the Manage Monitor Collections page you should enter a unique name and select at least one monitor from the list below in order to create a collection (a group).

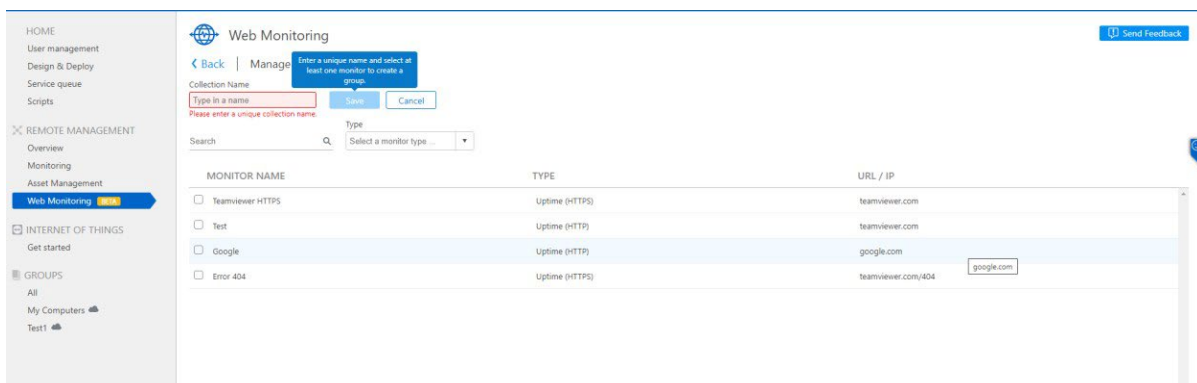


Image: Adding monitor collection 2

Your added Monitor Collections will be visible on the left side in the list and on the right side of the selected collection the monitors included in the collection will be reflected.

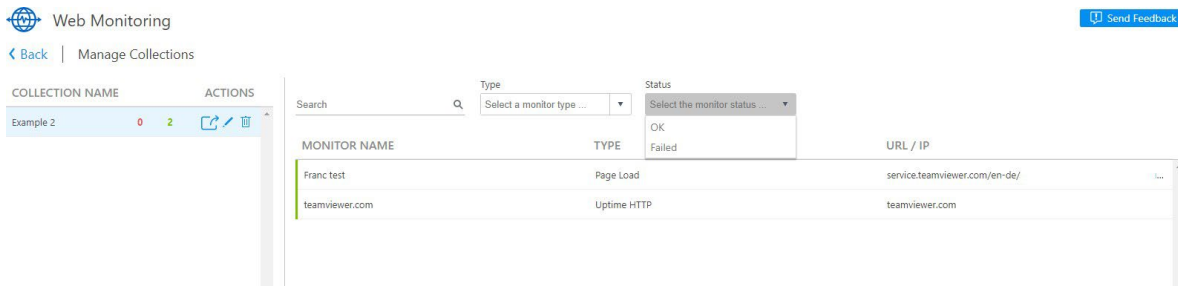


Image: The list of monitor collections

You can easily add another Monitor collection and include existing monitors in it by clicking the + button at the bottom of the page.

Monitor Collections provides you with an overview possibility on your collections. It helps you to understand the number of monitors in each collection, the status of the included monitors and enables you to filter the monitors within the collections.

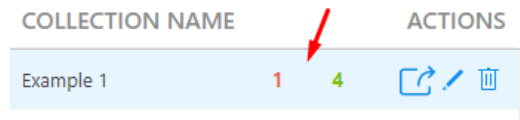


Image: Monitors overview in the collection

8.5.2. User Management

In the TeamViewer Management Console, there are 3 levels of users, Company Administrators, User Administrators and Users.

As a Company Administrator or User Administrator you can create both monitors and collections and share them with regular Company Profile Users.

Company Administrators and User Administrators can see everything related to the Web Monitoring service once they log in to the TeamViewer Management Console. They can create, edit or delete individual monitors or entire collections of monitors. They can also share or unshare collections with other users inside the company profile.

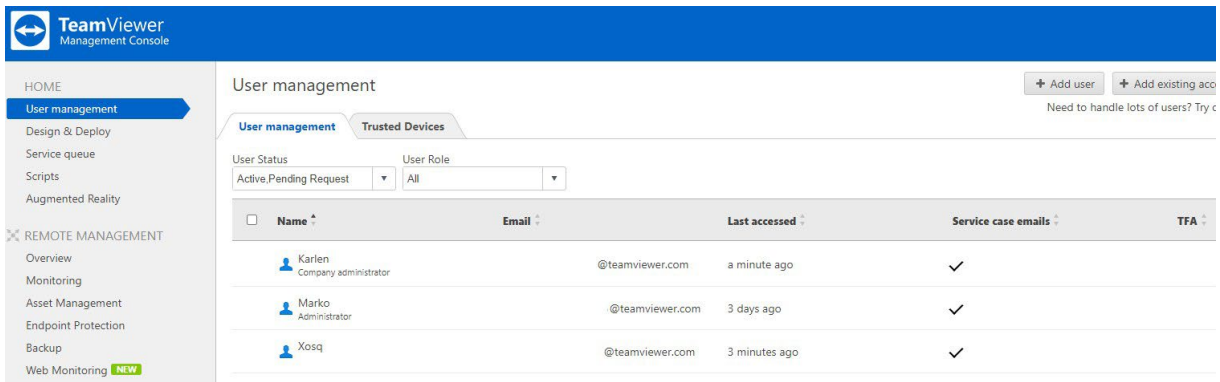


Image: User management levels

User Management helps customers to limit who can see and who can create or delete monitors or collections of monitors inside the company.

8.5.3. Sharing Monitor Collections

The monitor collection can be shared with Company Users. Once shared with them they will be able to see the Web Monitoring dashboard in the TeamViewer Management Console. This includes having access to the monitors listed in the collection, their charts, and associated alarms. A company user will only be able to edit the monitors which are part of the shared collection.

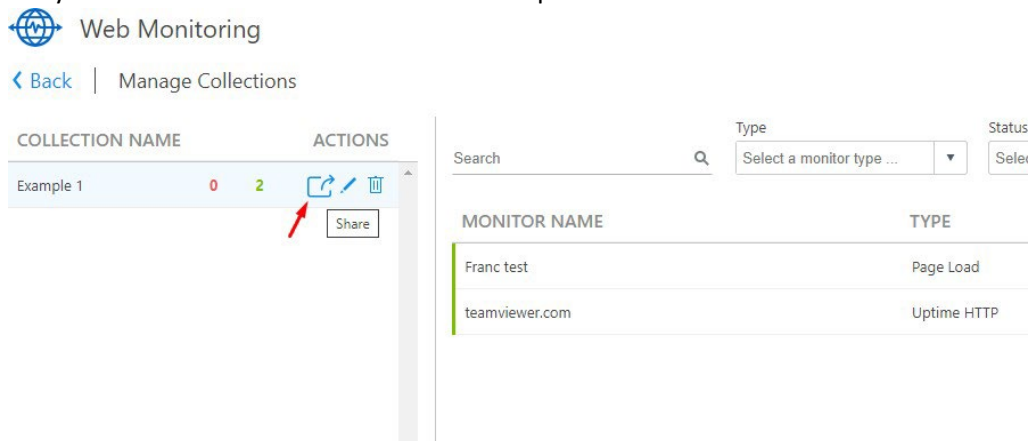


Image: Sharing the collection

The monitor collection sharing and user management features allow TeamViewer Web Monitoring to be more efficient and customers who have multiple colleagues that are monitoring web resources can now distribute the workload with the sharing capability.

8.6. Data exporting

You can also export your monitor's historical data to a csv file for later usage. Simply click the Export CSV button from the monitor's Chart View module submenu. The CSV file will automatically download to your Local drive.

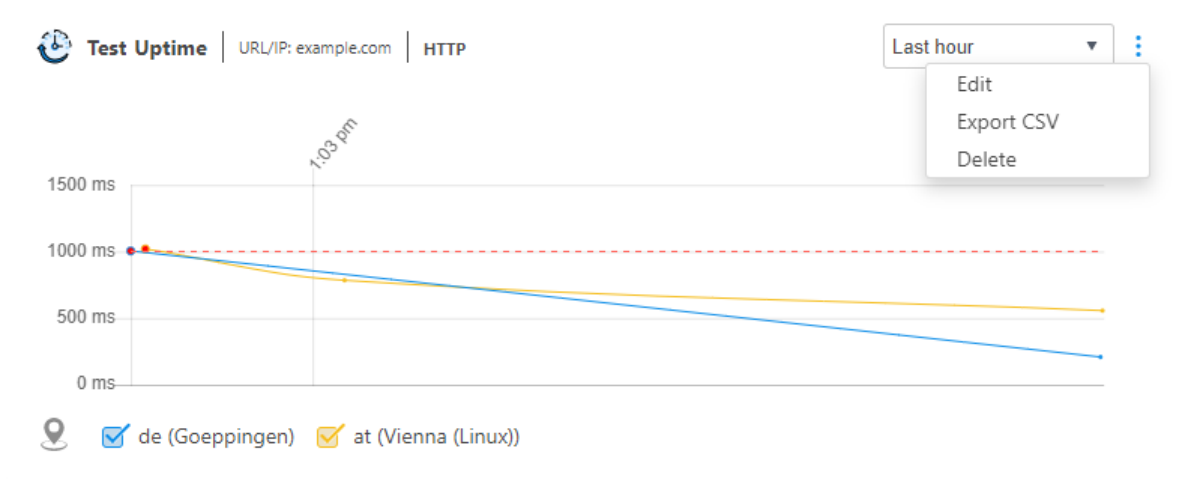


Image: Data exporting

8.7. Web Monitoring API

Our web-based API allows you to access data and control various aspects of their TeamViewer account. You can use the API to develop apps that integrate TeamViewer functionality into own corporate environment or can develop apps that everyone can use.

The API uses REST to communicate with the application and the secure authorization standard OAuth 2.0 to manage access to data.

For more details see the [Develop Custom TeamViewer Solutions](#) web page and the API

Documentation - <https://webapi.teamviewer.com/api/v1/docs/index#/>

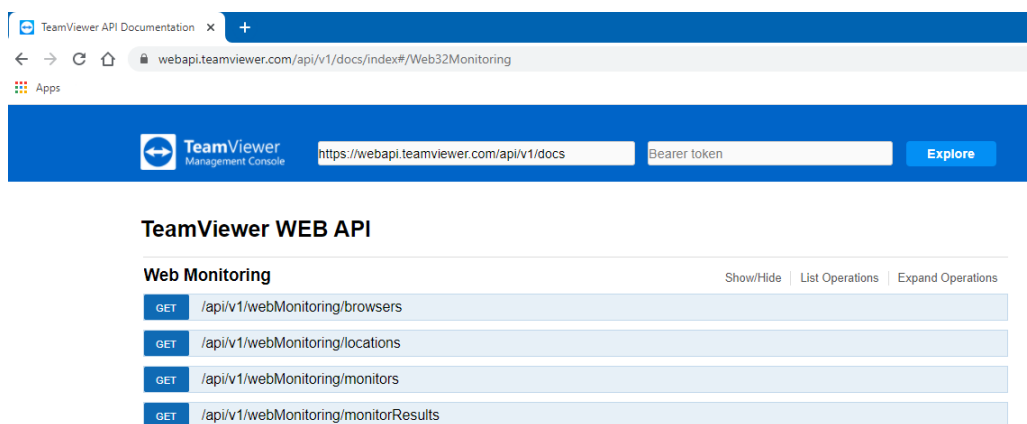


Image: Web API

8.7.1. Web Monitoring - API Actions

1. **GET Browsers** action is used to get the list of supported Browsers. Currently the API action, as now support 1 browser version, returns only Browser types and Id, the versions will come soon.
2. **GET Locations** action is used to get the list of supported Locations, it returns location Id, continent, country, and city names.
3. **GET all Monitors list** action is used to get the list of all monitors with configuration details that are available on the account.
4. **GET Monitor result** action is used to get the specified monitor results for the specified date and/or interval.
5. **GET Alarms data** action provides the alarm's type, location IDs, status (Raised, Resolved or Acknowledged), duration, resolving or being acknowledged time and in some cases the response time for the specified monitor.

9. Contact book and Integrations

There are many ways to notify you about the fact that an alert has occurred in TeamViewer Remote Management (TV RM).

The default notification types are phone call, SMS, and email messages. TeamViewer Remote Management has also developed integrations with third party systems, such as Webhook, and others will be added soon.

Contact book is general notification center for Remote Management, and it allows you to create different contact types and use them as channels to organize the notification process for their Remote Management services.

Contact book is currently available for Web Monitoring and can be get by clicking the corresponding button at the top right corner of Web Monitoring Tab.

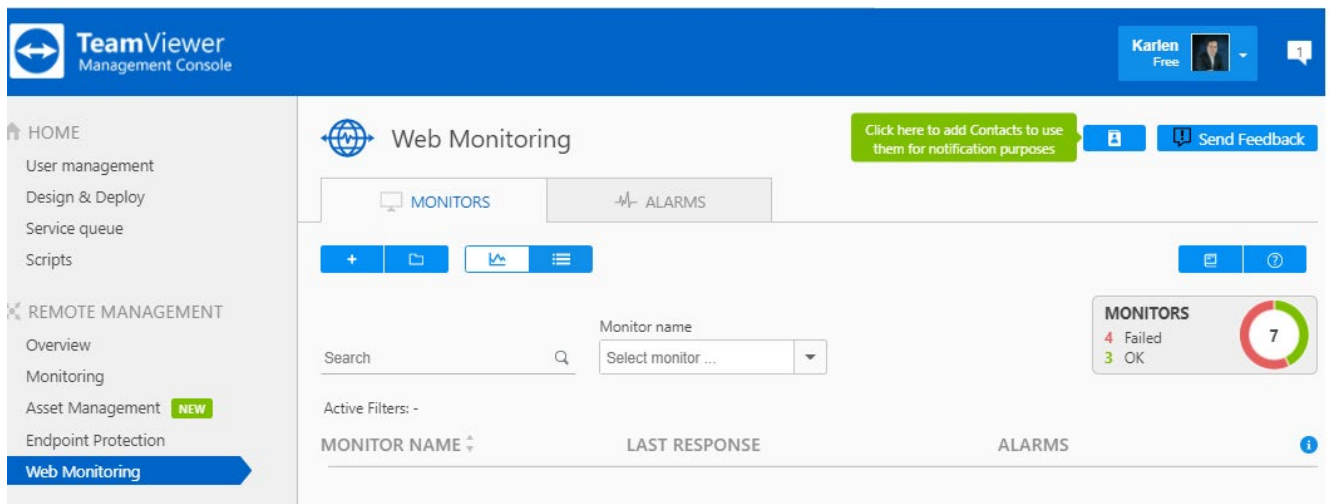


Image: Contact book button

CONTACT GROUP(S)	ACTIONS		
<div style="display: flex; justify-content: space-between; align-items: center;"> + <div style="text-align: right;"> Contact Type Select contact type ▼ </div> </div>			
Search <input type="text"/>			
Active Filters: -			
CONTACT NAME / ALIAS ↕	STATUS ↕	CONTACT GROUP(S)	CONTACT TYPE ↕
For Testing External Groups	Active	-	Webhook
Ka	Active	-	Email
Karl	Active	-	Email
Test 19.05 - ext	Active	-	Email
Testing	Unconfirmed	-	Webhook

Image: Contact book

9.1. TeamViewer Contacts

You can add TeamViewer contacts from your Computers and Contacts list as Remote Management contacts and use them for notification purposes.

All you need to do is to select the needed contact from Contact name's field drop down list and click Add, this will create an email Contact type by using the email address that is already kept in TeamViewer.

Add contact
✕

Select "TeamViewer contact" to create a contact based on the existing email address available in TeamViewer or provide a different email address by selecting "External contact". Contacts can be used for alarms notification purposes.

Contact Type

TeamViewer contact
 External contact

Contact name

Cancel
Add

Image: Adding TeamViewer contacts

The created TeamViewer contact can be used to get alarm and recovery notification emails for example when Web Monitoring monitor threshold triggers.

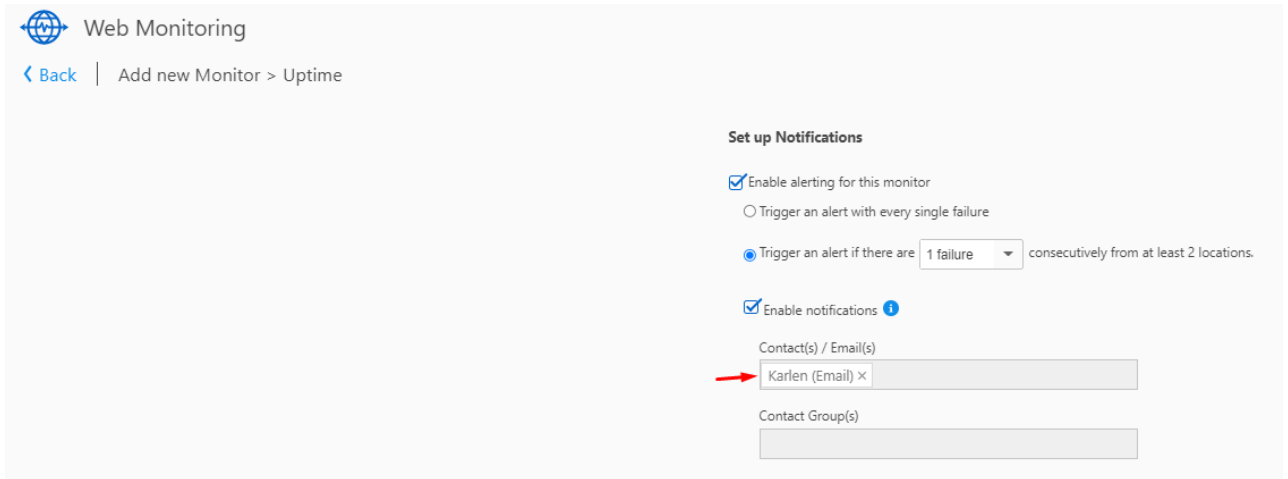


Image: Usage of a TeamViewer contact in the monitor notifications config

9.2. External Contacts

You can add external contacts (people without a TeamViewer account) into the Contact Book and use those contacts for notification purposes.

External contacts can be added by clicking the Add Contact button in the Contact Book and by selecting the "External contact" option.

This time you should provide a unique contact name and a valid email address. A corresponding confirmation link would be sent to the provided email address.

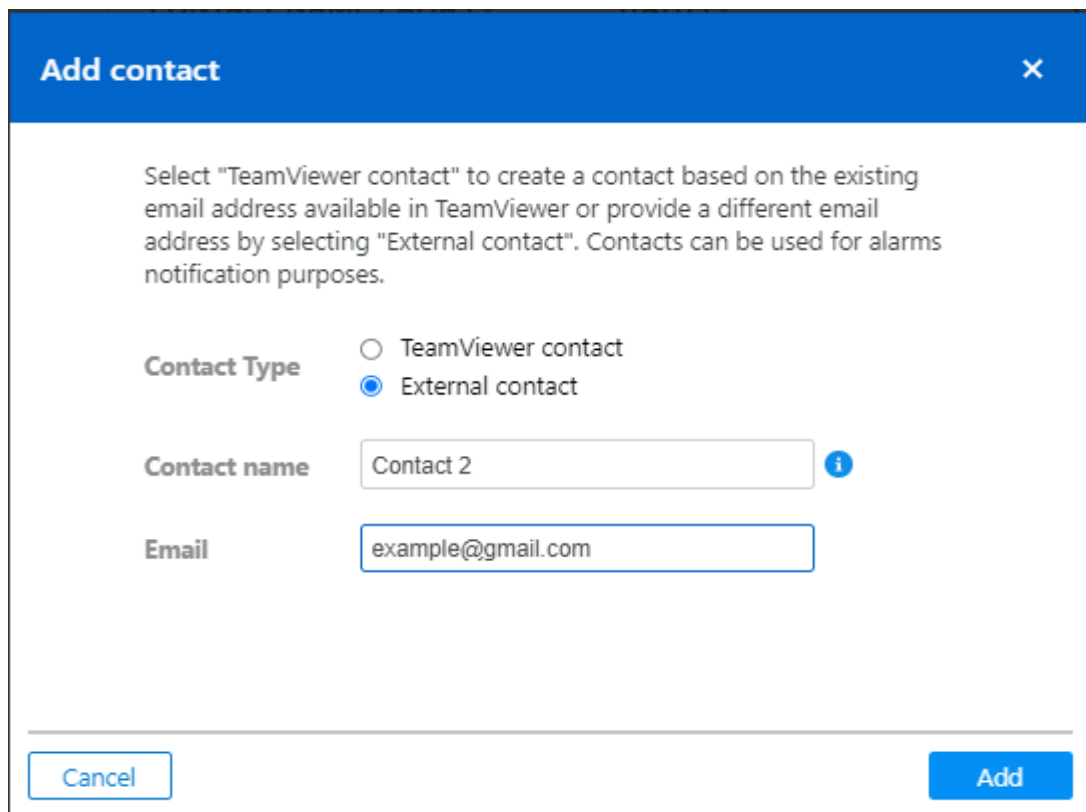


Image: Adding external contacts

notification emails.

9.3. Contact groups

Group of Contacts helps you organize contacts to a particular group to receive alerts and notifications. Contact groups make notification process management more effective; groups are used to send notifications to multiple people when an alert is triggered. Changes to a Contact Group (e.g., adding or removing people) are much faster than e.g., changing the alert recipients for many different monitors one by one.

You can create a group of contacts by clicking the + button in the left bottom part of the Contact Book and by selecting the contacts to be added to the Group.

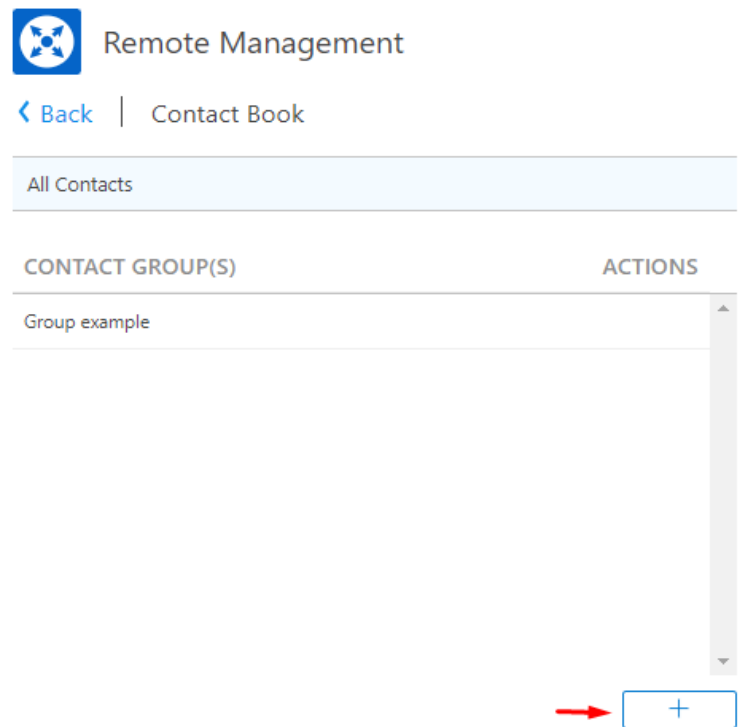


Image: Add Contact group button

All Contacts

CONTACT GROUP(S) ACTIONS

CONTACT NAME / ALIAS	STATUS	CONTACT TYPE
<input checked="" type="checkbox"/> Contact 4	Active	Email
<input checked="" type="checkbox"/> Contact Webhook 3	Active	Webhook
<input type="checkbox"/> Contact 1	Unconfirmed	Email
<input checked="" type="checkbox"/> Contact 2	Active	Email

Group name:

Contact Type:

Image: Creating a Contact group

Remote Management

< Back | Contact Book

All Contacts

CONTACT GROUP(S) ACTIONS

CONTACT NAME / ALIAS	STATUS	CONTACT TYPE
Contact 4	Active	Email
Contact Webhook 3	Active	Webhook
Contact 2	Active	Email

Group example

Image: Contact group

You can select which Contact types (e.g. Email, Webhook) included in the group should be used for notifications.

Web Monitoring

< Back | Edit uptime monitor > Teamviewer

Set up Notifications

Enable alerting for this monitor

Trigger an alert with every single failure

Trigger an alert if there are consecutively from at least 2 locations.

Enable notifications ⓘ

Contact(s) / Email(s)

Contact Group(s)

- Group example (Webhook)
- Group example (Email)

Going forward, the Contacts and the Contact Groups will also be used in the Reporting functionality.

9.4. Integrations

9.4.1. Webhook

What is a webhook?

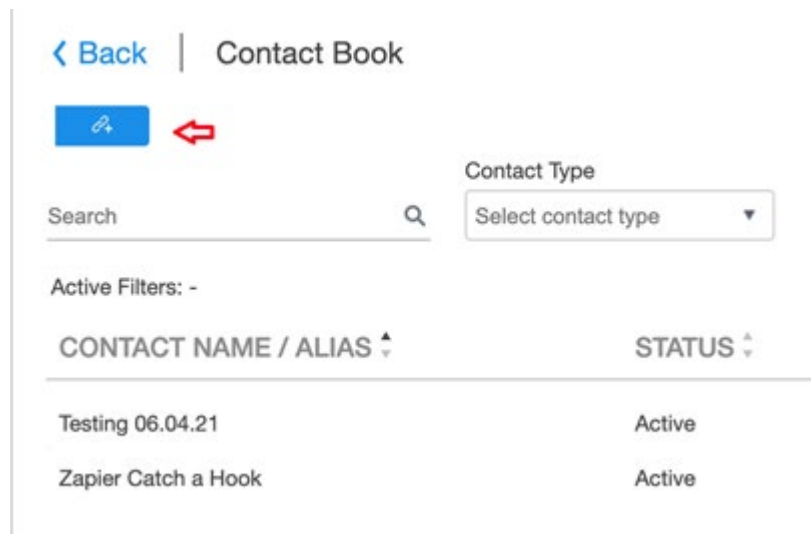
A webhook is a HTTP POST JSON format request that TeamViewer Remote Management sends to the URL of your choosing when a certain alert occurs. This request is accompanied by a payload of data in the body of the POST directly related to the alert. A webhook with a state change is triggered when a monitor or a check changes its state from OK to Failed and the opposite as well.

With webhooks it is easy to connect your TV RM alerts data with multiple applications. Webhooks work on an alert-based output mechanism. It allows you to streamline and manage your critical TV RM alerts in almost any third-party application.

How to setup?

To setup a webhook integration it requires you to first **get a Webhook URL** of the desired third-party service. **Once you have the Webhook URL**, follow the steps below to integrate TV RM alerts data with other third-party applications using Webhooks:

1. Log in to the TeamViewer Management Console - <https://login.teamviewer.com/LogOn>
2. Navigate to Remote Management > **Web Monitoring** > **Contact Book** > **Add Integration**



3. Select **Webhook** in the integration types drop-down list
4. Add the Alias and provide the Hook URL
5. Click Add

6. Confirm the Webhook by entering the 6-digit confirmation code

Now you have a new Webhook contact that will allow a connection to another third-party application.

CONTACT NAME / ALIAS	STATUS	CONTACT TYPE
Testing 08.04.21	Active	Webhook
Phone Calls a hour	Active	Webhook

How to use webhooks?

If you are connecting to a third-party system, the third-party system is expecting the incoming Webhook (e.g., the data sent from your app to that system) to use a message format to process it.

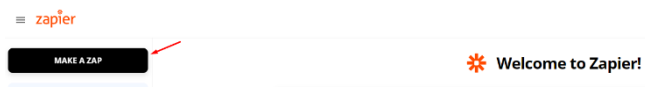
If you already have a Webhook contact, you can now configure your Webhook alerts to integrate your Remote Management solution with other third parties by using a service like [Zapier](#).

Zapier

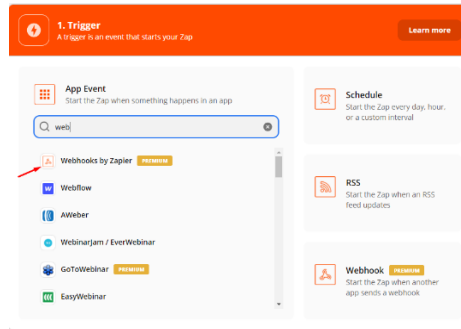
Zapier is a universal application that allows a connection to thousands of web apps by creating **Zaps**. Zap is a workflow that connects apps, so that they can work together. Zaps join multiple third-party apps by enabling a trigger and an action; finally, it helps to automate tedious tasks throughout the workflow.

How to set up a Zap

1. Log in to your Zapier
2. Click on the **Make a Zap** button



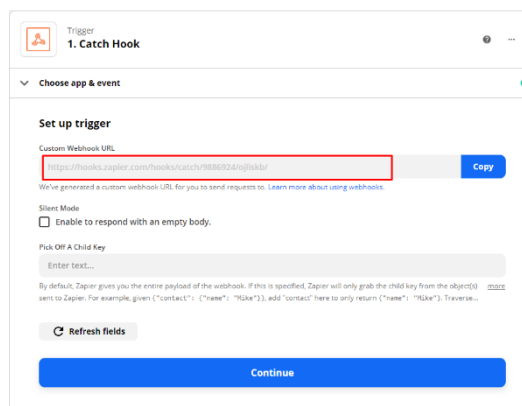
3. Select **Webhooks by Zapier** from the list of supported apps



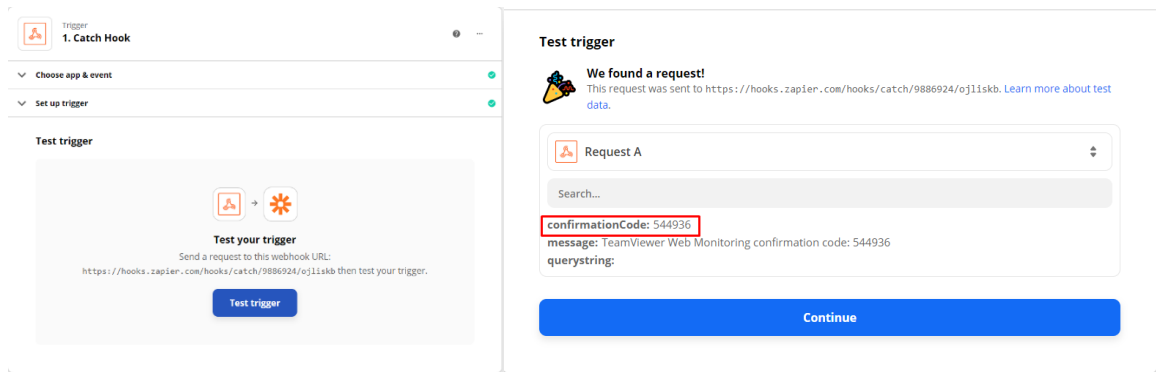
4. Select **Catch Hook** or **Catch Raw Hook** and click Continue



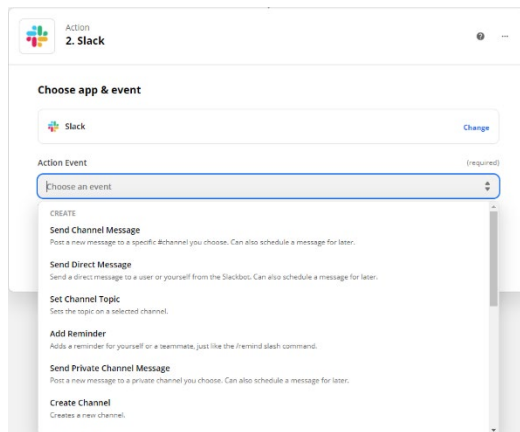
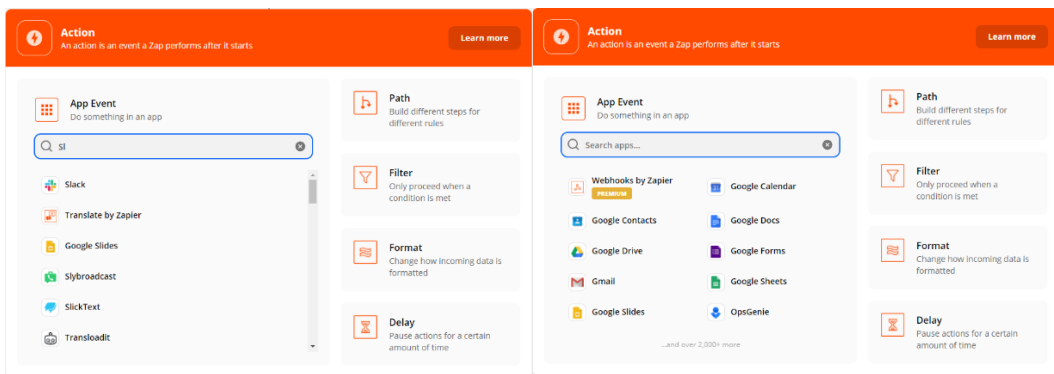
5. Copy the custom Webhook URL and use it to set up a Webhook contact in the Remote Management Contact Book – (see **How to setup?** section above)



6. Click the **Test your trigger** button to get the 6-digit confirmation code to use to activate the Webhook contact



7. Now that you have an active Webhook contact which is already connected with a Zap, you can select the third-party app you want to push your alert messages to, for example Slack or others.



Examples of Webhook JSON output

```
{
  "AlarmStart": "2021-Apr-04 17:48:50 UTC",
  "Details": "Given remote host could not be resolved",
  "FailuresFrom": "DE (Munich), AT (Vienna)",
  "MonitorCollections": "Test Monitor Collection",
  "MonitorName": "Daniel' Sensor",
  "MonitorType": "Uptime",
  "Protocol": "HTTP",
  "RequestMethod": "GET",
  "URL": "http://sdifvndafgfaudnsnfd.com"
```

}

10. Reporting

10.1. Web Monitoring reports

The Reporting for Web Monitoring allows you to create ad-hoc and recurring reports which will be sent to email contacts (see [Contact book](#)) on scheduled monthly, weekly, or daily basis.

You also have possibility to download the created reports and to use them later according to your needs.

Ad-hoc reports

Ad-hoc or One-time reporting is a process in which dynamic, real-time data reports are created for a custom date range by the user on an as-needed basis. They are designed to answer a specific business question, usually in response to an event.

To create an Ad-hoc report, you need to click the Create reports button at the top-right corner of the screen and start the simple 1-step configuration.



Image: Create a report

Select the custom date range, report format and the affected monitors to generate the report.

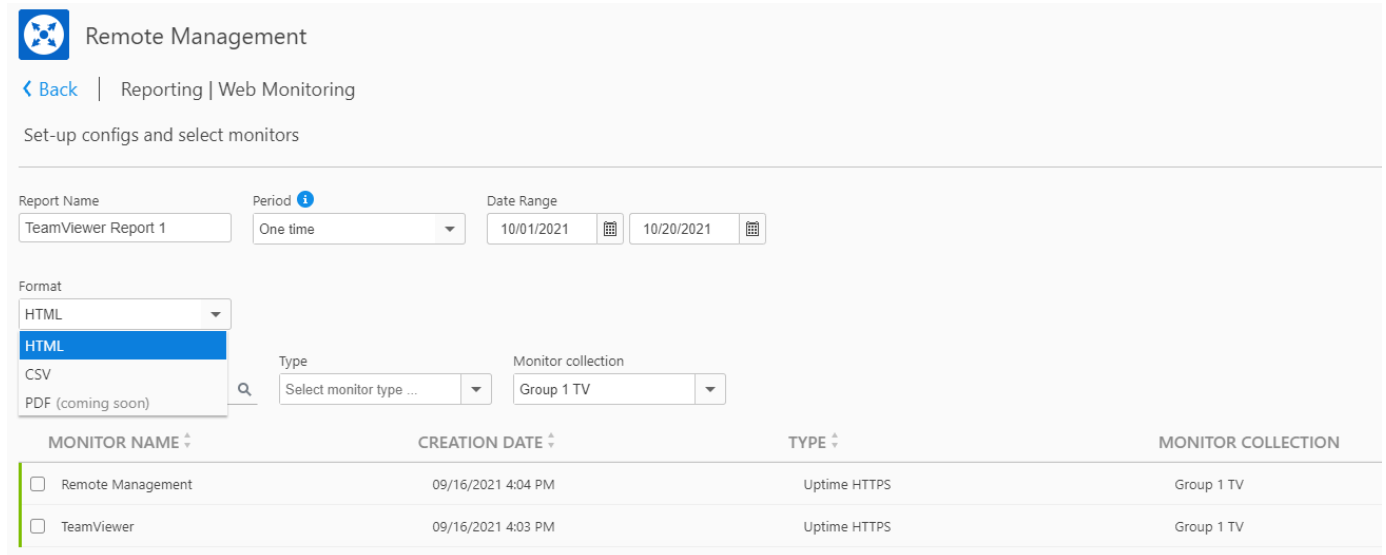


Image: Ad-hoc(One-time) report configuration

Navigate to the created report and download it by clicking the corresponding button at the right corner.

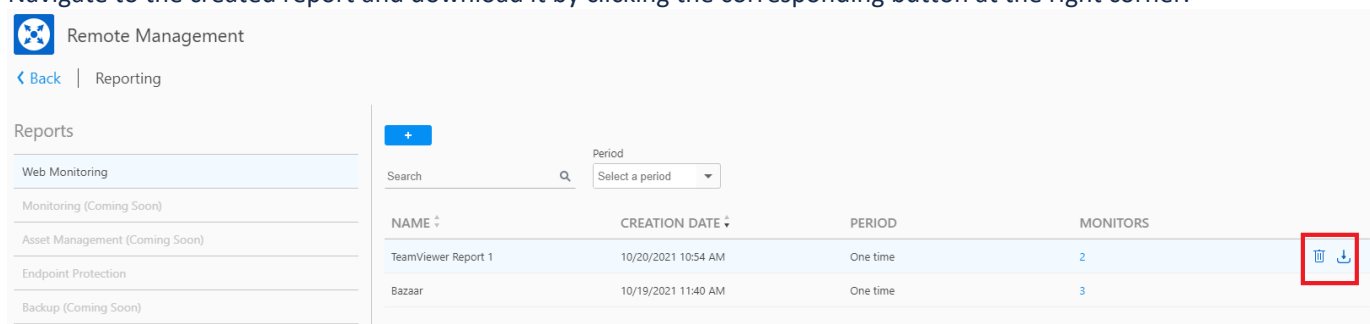


Image: Ad-hoc (One-time) report deleting and downloading

Scheduled email reports.

By selecting Monthly, Weekly, or Daily from periods drop-down list you can create scheduled reports and get those reports via email on recurring bases.

For example, monthly reports when generated will be available and sent to the corresponding, selected during configuration email contacts, on the first day of the next months.

To create a recurring report, you need to configure the reports main parameters like format and monitors on step 1 and also select email contact(s) on step 2 to whom those reports will periodically be sent via email.

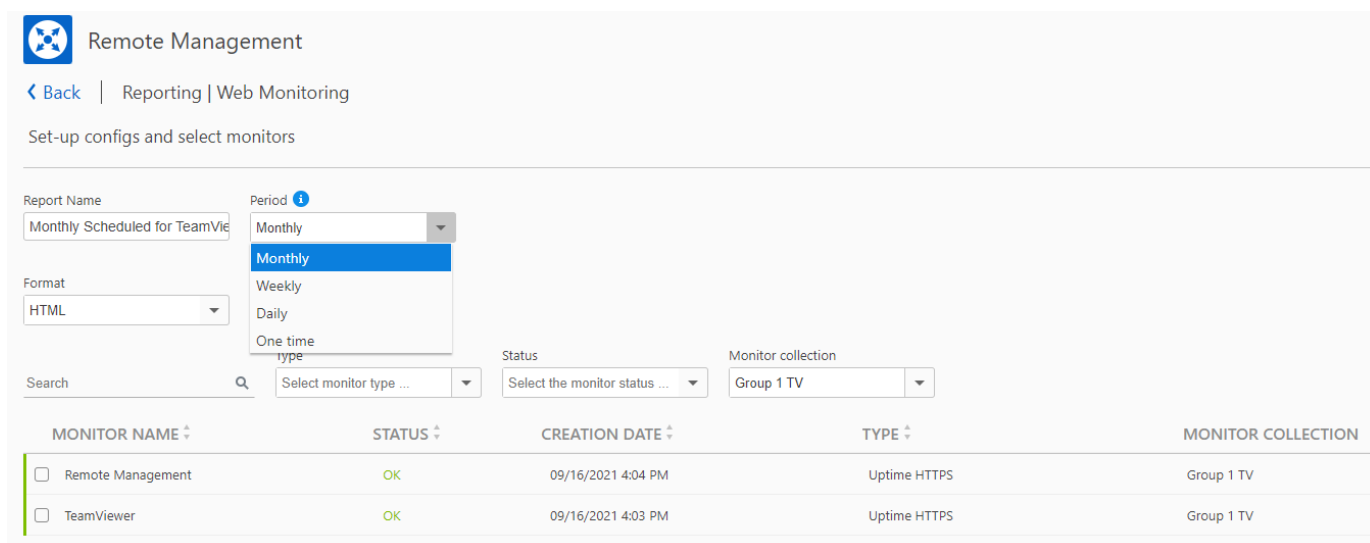


Image: Scheduled) report configuration – step 1

Select the monthly, weekly, or daily period, report format and affected monitors to generate the report and on the next step select the email contacts who will start getting the periodic reports.

Remote Management

< Back | Reporting | Web Monitoring

Step 2: Select contact(s) ⓘ

Search Contact

CONTACT NAME	CONTACT GROUP(S)
<input type="checkbox"/> [Redacted]	-
<input checked="" type="checkbox"/> [Redacted]	-

Image: Email contact(s) selecting – step 2

11. Support

For questions, additional assistance, and support, please contact our experienced support team by [submitting a ticket](#). You can also visit our [Community](#) page for further support. We are always happy to help!

V10.01.01.2201

TeamViewer Germany GmbH
Bahnhofplatz 2
73033 Göppingen
Germany

©2022 TeamViewer Germany GmbH. All rights reserved.