TeamViewer 10 Manual

ITbrain

Rev 10.2-201503

Table of contents

1 General

1.1 About ITbrain™

ITbrain™ is a simple and professional IT management platform that is integrated into TeamViewer. The following services are available for ITbrain™:

- ITbrain™ Monitoring and Asset Management
- ITbrain™ Anti-Malware

With ITbrain™, TeamViewer, and the TeamViewer Management Console, you'll maintain a clear overview of all the important information and functions of your system.

- With the **ITbrain**™ **Remote Monitoring and Asset Management** service, you can set up individual checks to receive notifications e. g. disk health, antivirus software, online status, RAM use, or running processes on a computer. The built-in asset tracking feature also lets you create IT inventory reports for your network. Manage all your devices conveniently via the TeamViewer Management Console or your TeamViewer Client and receive direct email alerts.
- With the **ITbrain**™ **Anti-Malware** service, you can protect your device from malware. ITbrain™ scans your devices on a regular basis. Discover potential threats early and protect your devices reliably. Discovered malware is killed immediately and can later be deleted completely. With the TeamViewer Management Console, you can manage all threats and scans at a glance - any time, anywhere.

Note: ITbrain™ supports computers with Windows XP SP2 or later and servers with Windows Server 2003 or later.

Note: ITbrain™ is not part of the TeamViewer license. Separate licenses are required to use all the features of ITbrain™.

1.2 About the manual

This manual describes how to work with ITbrain™ from TeamViewer.

Unless stated otherwise, the functionalities described always refer to the TeamViewer full version for Microsoft Windows. "ITbrain™" appears below simply as "ITbrain".

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, Microsoft, and Outlook 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, and Microsoft® Windows® 8 simply as “Windows”. For a list of all supported operating systems, visit our website at *http://www.teamviewer.com/en/kb/38-Which-operating-systems-are-supported.aspx*.

2 Requirements

The requirements that must be met in order to use all the functions of ITbrain are described below.

2.1 Licensing

ITbrain is a standalone product and is not included in the TeamViewer license model. This means that:

- ITbrain is not part of the TeamViewer Corporate, Premium, or Business license.
- ITbrain can be used even without a TeamViewer Corporate, Premium, or Business license.
- You'll need an ITbrain license in order to use all the functions of ITbrain.

ITbrain is available as a monthly or annual subscription. Under the ITbrain license model, you purchase a so-called "end-point" for each computer on which you want to use ITbrain. For example, if you want to monitor five computers with ITbrain, you'll need an ITbrain license with five end-points.

For more information about the ITbrain license model, visit our **ITbrain shop** under *https://www.itbrain.com/pricing/*.

Note: You can also try ITbrain for 14 days with no license or obligation to subscribe.

Note: You will need different end-points for each ITbrain service. The different end-points can be used independently of oneanother.

2.2 System requirements

To view alert messages of ITbrain, you will need the TeamViewer Management Console.

The TeamViewer Management Console is browser-based and is thus independent from the operating system.

Alternatively, you can use the TeamViewer 9 full version (or later) with the following operating systems:

- Windows
- Linux
- iOS
- Windows Phone 8

2.2.1 ITbrain Monitoring and Asset Management

To use ITbrain Monitoring and Asset Management, one of the following operating systems must be running on the devices (end-points) you wish to monitor:

- Windows 8 / 7 / Vista / XP SP3
- Windows Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 R2
  The antivirus software check is not supported for server operating systems.

TeamViewer 8 full version or Host (or later) must also be installed.

2.2.2 ITbrain Anti-Malware

To use ITbrain, one of the following operating systems must be running on the devices (end-points) you wish to protect using ITbrain Anti-Malware:

- Windows 8 / 7 / Vista / XP SP3
- Windows Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 R2

TeamViewer 9 full version or Host (or later) must also be installed.

3 Configuring ITbrain

You can use the TeamViewer Management Console to configure ITbrain for use. 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 ITbrain are described below.

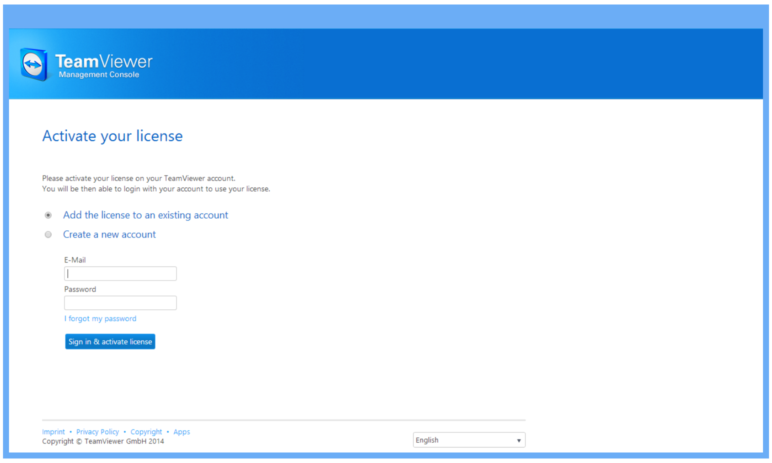
> **Note**: Depending on assigned permissions, TeamViewer accounts set up under your company profile can also use the functions described below.

3.1 License activation

As described in *Section 2.1 "Licensing", page 6*, you need an ITbrain license in order to use all the functions of ITbrain. After you purchased an ITbrain license, you'll receive a confirmation email.

- Click on the activation link to activate the license for your TeamViewer account.

Once you haveve activated the license, it will be linked to your TeamViewer account and is ready to use.



TeamViewer
Management Console

Activate your license

Please activate your license on your TeamViewer account.
You will be then able to login with your account to use your license.

● Add the license to an existing account

○ Create a new account

E-Mail

Password

I forgot my password
Sign in & activate license
Imprint • Privacy Policy • Copyright • Apps

Copyright © TeamViewer GmbH 2014

Activating an ITbrain license for your TeamViewer account.

Note: If you set up your TeamViewer account under a company profile, the ITbrain license will be usable at the company level.

Note: ITbrain license activations can only be undone in exceptional cases.

3.2 Activating ITbrain for end-points

All computers on which you want to use ITbrain are called end-points. ITbrain must be activated and configured on each end-point. You can use bulk activation to activate ITbrain on multiple devices at the same time, or activate ITbrain on each end-point separately.

After activating ITbrain Anti-Malware on the end-points, the following steps are proceeded automatically:

- The ITbrain service is downloaded and installed on the device.
- The latest ITbrain virus definitions are downloaded.
- A quick scan is started.
- The Default Anti-Malware policy is assigned to the device.

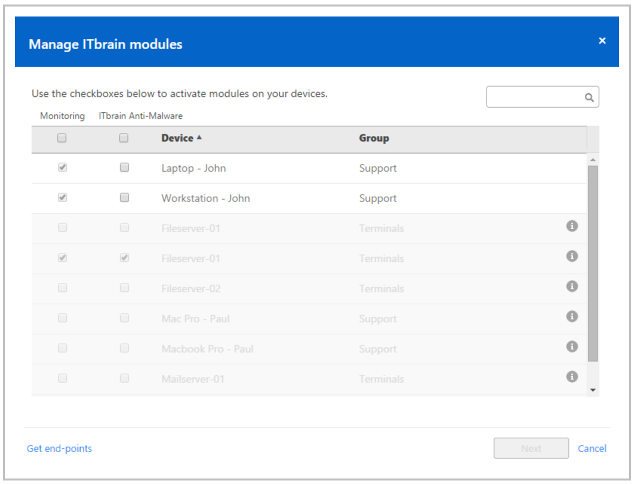
3.2.1 Bulk activation

Bulk activation lets you activate ITbrain on multiple end-points and assign all of them to your TeamViewer account collectively. By using your personal passwords, all end-points are automatically assigned to your account and ITbrain is activated for the end-points in one step.

Bulk activation can be accessed in one of the following ways:

- ➡ Under **ITbrain | Alert Report**, click the **Add devices** button.
- ➡ Select a device group from your Computers & Contacts list and click **Tools | Monitor devices with ITbrain**.

In the dialog, select the ITbrain services you would like to use for the respective devices. Then follow the instructions in the dialog.



Manage ITbrain modules

Use the checkboxes below to activate modules on your devices.

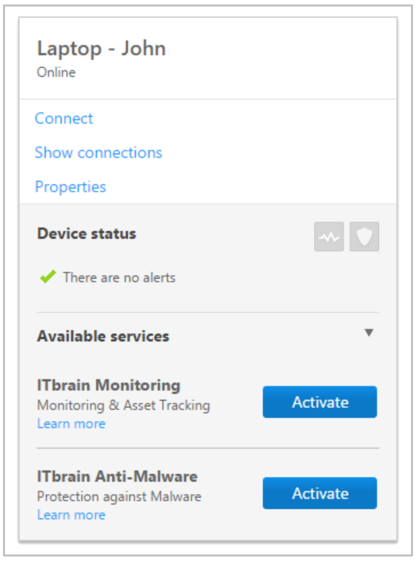
Monitoring □	ITbrain Anti-Malware □	Device ▲	Group
☑	□	Laptop - John	Support
☑	□	Workstation - John	Support
□	□	Fileserver-01	Terminals
☑	☑	Fileserver-01	Terminals
□	□	Fileserver-02	Terminals
□	□	Mac Pro - Paul	Support
□	□	Macbook Pro - Paul	Support
□	□	Mailserver-01	Terminals

Bulk activation for all ITbrain end-points.

3.2.2 Activating end-points separately

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

- To do this, click the device name in your Computers & Contacts list, then select **Activate** for the respective service.



Laptop - John
Online

Device status

✓ There are no alerts

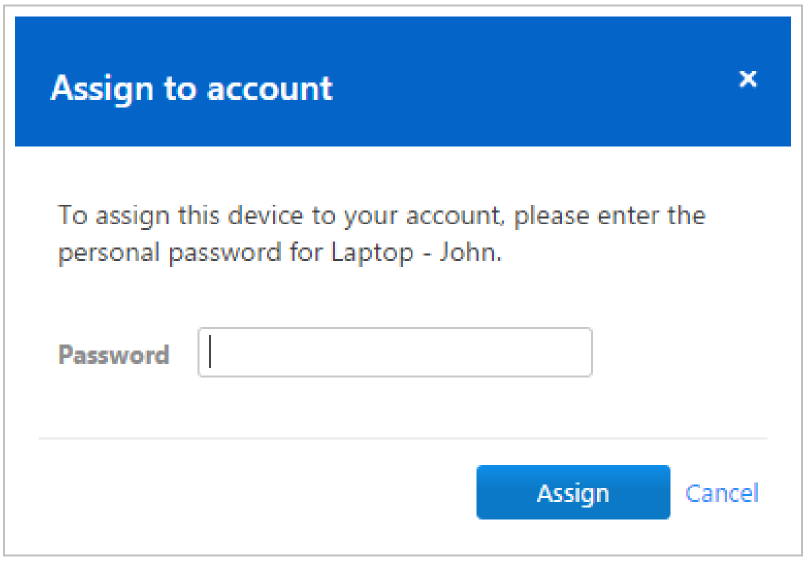
Available services

ITbrain Monitoring
Monitoring & Asset Tracking

ITbrain Anti-Malware
Protection against Malware

Activate ITbrain for individual end-points.

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



Assign to account

To assign this device to your account, please enter the personal password for Laptop - John.

Password

Assigning a device to your account using your personal password.

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

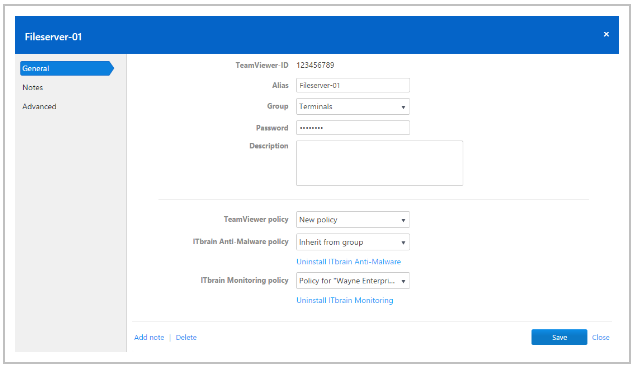
➡ To do so, you'll need to access the settings locally on the computer under **Extras | Options | General | Account assignment**.

3.3 Assign an ITbrain policy to an end-point

Define policies that determine to what extent and when the computers are checked for malware or errors.

The product comes with a default policy already preconfigured for each service.

Policies can also be assigned to a group. In this case, all end-points within the group will inherit the policy. In order for this to occur, **Inherit from group** must be selected for each end-point within the group.



Fileserver-01

TeamViewer-ID 123456789

Alias Fileserver-01

Group Terminals

Password ••••••••

Description

TeamViewer policy New policy

ITbrain Anti-Malware policy Inherit from group

ITbrain Monitoring policy Policy for "Wayne Enterpri...

Assign an ITbrain policy to an end-point.

In the last step of the configuration process, you will assign one of the available policies to the end-point.

➡ Click on the name of the end-point in the Computers & Contacts list, then select **Properties**. In the properties of the end-point, select a configured policy under **ITbrain Monitoring policy** and **Anti-Malware policy**.

➡ Alternatively, select a policy during the bulk activation process or assign a policy to a group.

The **Inherit from group** policy is selected by default for all end-points and the **Default policy** is assigned by default to all groups. To learn how to configure your own policy, see *Section 3.3.1 "Configuring policies", page 12*.

The **default monitoring policy** includes the following checks, which are described in *Section 3.3.1 "Configuring policies", page 12*:

- 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?

The **Default Anti-Malware policy** includes the following scans, which are described in *Section 3.3.1 "Configuring policies", page 12*:

- Quick scan, daily 09:00 AM
- Full scan, daily at 12:00 PM

3.3.1 Configuring policies

Define policies for each ITbrain service. Depending on the service, it contains the following information:

- **Anti-Malware policies**: Determine when and to what extent your devices are scanned for malware by ITbrain Anti-Malware.
- **Monitoring policies**: Determine according to what criteria your devices are checked by ITbrain Monitoring and Asset Management.

All policies are listed under **ITbrain | Policies**. You can create new policies there as well.

➡ To create a policy, click the **Add policy...** button.

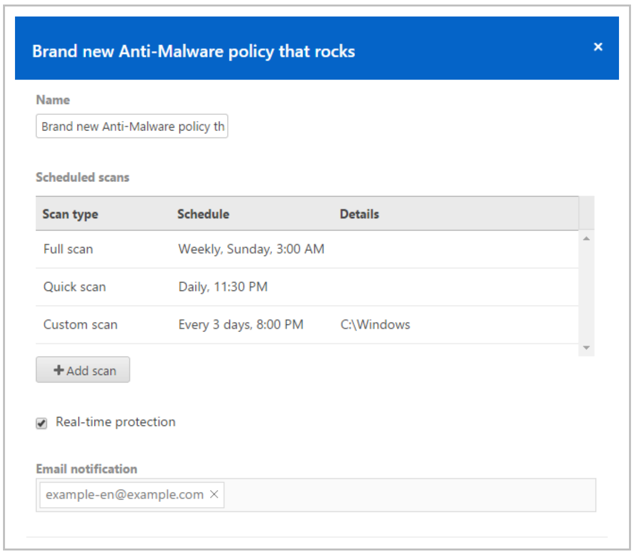
The following is a brief example of how different policies can be used.

> ***Example***: *Define different policies depending on the hardware used. For example, you want to make sure that a particular service is always running on your servers. Receive an alert whenever the service stops running. You also wish to ensure that Windows Update is activated*

on all your monitored desktop computers. Receive a notification whenever Windows Update becomes deactivated.

3.3.2 Add a new policy

In this dialog, you can select a **name** for the policy and define necessary options for each policy. The options available for each policy are described below.



Brand new Anti-Malware policy that rocks

Name: Brand new Anti-Malware policy th

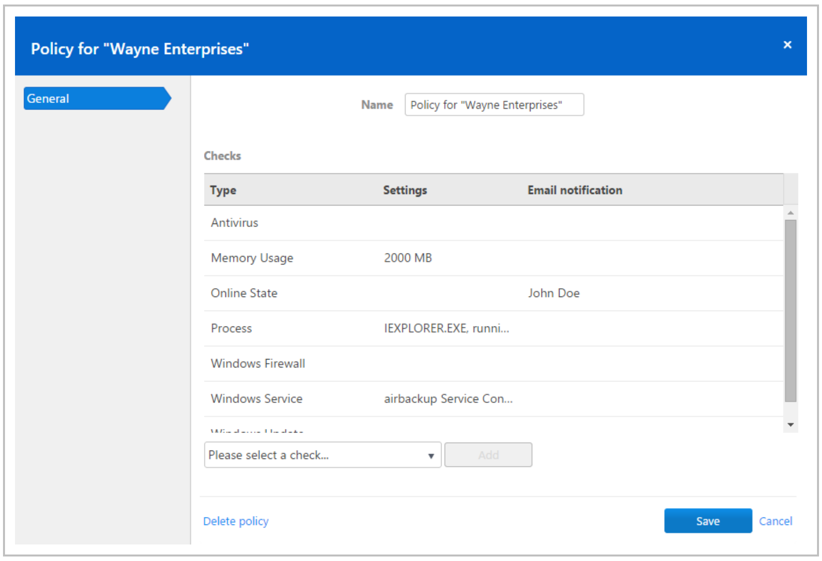
Scheduled scans

Scan type	Schedule	Details
Full scan	Weekly, Sunday, 3:00 AM	
Quick scan	Daily, 11:30 PM	
Custom scan	Every 3 days, 8:00 PM	C:\Windows

☑ Real-time protection

Email notification: example-en@example.com ×

Configuring an ITbrain Anti-Malware policy.



Policy for "Wayne Enterprises"

Name: Policy for "Wayne Enterprises"

Checks

Type	Settings	Email notification
Antivirus		
Memory Usage	2000 MB	
Online State		John Doe
Process	IEXPLORER.EXE, runni...	
Windows Firewall		
Windows Service	airbackup Service Con...	
Windows Update		

Configuring an ITbrain Monitoring policy.

Add an Anti-Malware policy

Scheduled Scans

Scans 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:

- **Quick scan**: ITbrain Anti-Malware will only scan certain data, running processes and the registry. This way, the scan is completed quickly and the most important data of your device are protected.
- **Full scan**: ITbrain Anti-Malware will entirely scan all hard drives of your devices. This scan will take longer than a quick scan. The device's data are entirely protected.

> **Note**: Please note that the speed of your system could be affected during the duration of a scan.

- **Custom scan**: ITbrain Anti-Malware will scan a defined hard drive, folder, or file. To do so, enter the path as follows: `C:\Folder\Filename.fileextension`.

Real-time protection

On/Off 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.

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

Email notification

Email If a threat is detected, ITbrain will send an email notification to the defined email adresses.

➡ Enter the email addresses that will receive notifications about detected threats.

Add a monitoring policy

ITbrain Monitoring Check	Description
Antivirus	Alerts you if no antivirus software is installed or the antivirus software is out-of-date.
Memory Usage	Alerts you if the average available RAM falls below the defined threshold for a period of time over five minutes. Enter the desired threshold in the input field.
CPU Usage	Alerts you if the average usage of a processor exceeds the selected threshold for a period of time over five minutes. Select a threshold using the slider.
Event Log	Alerts you if certain information is detected in an event log. The alert is triggered only if all the parameters described below are met. • **Name**: Enter a descriptive name. • **Event Log**: Select whether to check application, security, or system logs. • **Event ID(s)**: Determinethe event IDs of the logs for which you would like to be alerted. • **Event Source**: Define the event source. This lets you filter alerts by application, for instance. • **Event Type**: Select the event type (level) that will trigger an alert.
Disk Health	Alerts you whenever a disk reports physical errors. This applies to all internal hard drives.
Online Status	Alerts you whenever the device goes offline.
Process	Alerts you whenever a certain process is executed or not executed. • **Process name**: Enter the name of the process for which the alert will be triggered (e. g., BackupSC.exe). You can find the name via the task manager in the properties of the process under **Details | Original name**. • **Alert condition**: Select whether to trigger an alert whenever the process is ended or started.

ITbrain Monitoring Check	Description
Disk Space	Alerts you whenever the available hard drive space falls below the defined value. • **Disk**: Select the partition of the drive for which the alert will be triggered. • **Minimum free disk space**: Enter a value for the minimum available disk space. You will be alerted whenever the available disk space falls below the entered value.
Windows Update	Alerts you whenever Windows Update is deactivated.
Windows Service	Alerts you whenever a specified Windows Service is no longer running. • **Service name**: Enter the name of the service for which the alert will be triggered (e. g., airbackup Service Controller). You can find the name via the Windows Service Manager in the properties of the service under **General | Service Name.** • **Alert**: Select the number of checks with detected errors before you wish to be alerted.
Windows Firewall	Alerts you whenever the Windows Firewall is deactivated.

4 Monitoring

To monitor your devices and for asset management purposes, use the ITbrain service **ITbrain Monitoring**.

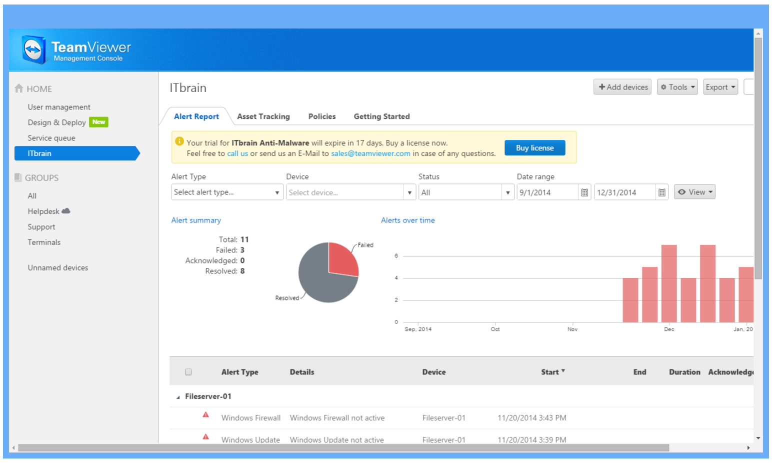
The devices configured according to *Section 3.2 "Activating ITbrain for end-points", page 9* are checked and monitored based on the policies (list of monitoring checks) assigned according to *Section 3.3.1 "Configuring policies", page 12*. Whenever all the defined conditions for a check are met, an alert is triggered and displayed as an alert message in the TeamViewer Management Console and the TeamViewer full version. An alert message indicates that a problem has occurred on one of the monitored devices.

4.1 Alert Report

Alert messages for every computer that has ITbrain installed are 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 ITbrain policies.

The **default monitoring policy** includes the following checks, which are described in *Section 3.3.1 "Configuring policies", page 12*:

- 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?



Your trial for **ITbrain Anti-Malware** will expire in 17 days. Buy a license now.
Feel free to call us or send us an E-Mail to sales@teamviewer.com in case of any questions.

Alert Type: Select alert type...
Device: Select device...
Status: All
Date range: 9/1/2014 – 12/31/2014

Total: **11**
Failed: **3**
Acknowledged: **0**
Resolved: **8**

	Alert Type	Details	Device	Start	End	Duration	Acknowledg
Fileserver-01							
⚠	Windows Firewall	Windows Firewall not active	Fileserver-01	11/20/2014 3:43 PM			
⚠	Windows Update	Windows Update not active	Fileserver-01	11/20/2014 3:39 PM			

Alert messages are shown in the Alert Report.

Alert messages are displayed in the TeamViewer Management Console for each computer that you are monitoring with ITbrain, should a check trigger an alert.

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

- In the sidebar, click **ITbrain** and select the **Alert Report** tab. Then select an **alert type**.
- In the sidebar, click on a group from your Computers & Contacts list and select the **Alert Report** tab. Then select an **alert type**.

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 by the according column. Using the **View** menu, you can define which columns should be displayed for the table and activate or deactivate the charts.

The status of the alerts is indicated by different icons.

Icon	Description
⚠	One of the defined checks has triggered an alert. The alert has not been acknowledged.
⚑	The alert has been acknowledged either by you or a contact with whom the computer has been shared.
✓	The issue that triggered the alert has been resolved.

4.2 Handling alert messages

If you know or can verify the cause of a monitoring alert and you would like to start troubleshooting the problem, you will first acknowledge one or more alerts.

To acknowledge monitoring alert messages, choose one of the following methods:

- Click the ⚙ ▾ icon next to an alert message and select the **Acknowledge** option.
- Select all the alert messages that you wish to acknowledge and click **Tools | Acknowledge selected.**

Once an ITbrain Monitoring alert has been acknowledged, you can troubleshoot the problem by connecting to the computer in question.

- To do this, click the ⚙ ▾ icon next to an alert message and select the **Go to computer** option. You can then connect to the computer as usual.

4.3 Checking alert messages

If you've solved the cause of the alert, you can use ITbrain to check whether the problem was successfully fixed and will not reoccur.

You can check alert messages in one of the following ways:

- Click the ⚙ ▾ icon next to an alert message and select the **Check now** option.
- Select all the alert messages that you wish to check and click **Tools | Check selected.**

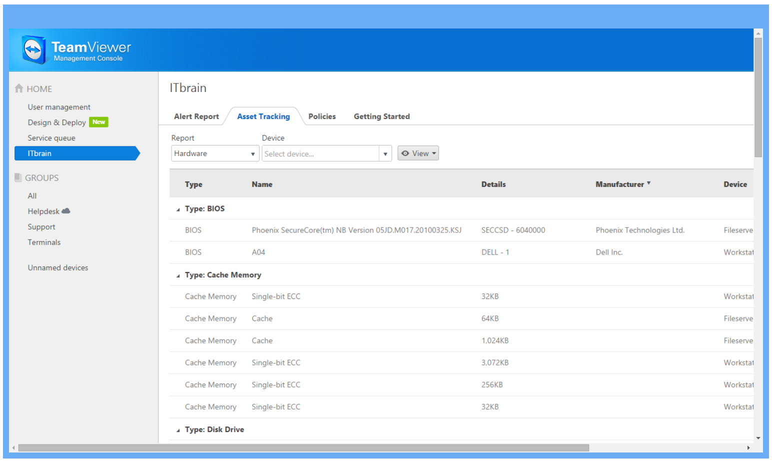
5 Asset Tracking

To monitor your devices and for asset management purposes, use the ITbrain service **ITbrain Monitoring**.

ITbrain also tracks the devices configured according to *Section 3.2 "Activating ITbrain for end-points", page 9* independently of its monitoring functions. Asset tracking gives you an overview of the components used in every computer on which ITbrain is used. The tracked devices are listed in the TeamViewer Management Console.

You can view the list of tracked components in one of the following ways:

- In the sidebar, click **ITbrain** and select the **Asset Tracking** tab.
- In the sidebar, click on a group from your Computers & Contacts list and select the **Asset Tracking** tab.



Report: Hardware

Device: Select device...

Type	Name	Details	Manufacturer	Device
Type: BIOS				
BIOS	Phoenix SecureCore(tm) NB Version 05JD.M017.20100325.KSJ	SECCSD - 6040000	Phoenix Technologies Ltd.	Fileserve
BIOS	A04	DELL - 1	Dell Inc.	Workstat
Type: Cache Memory				
Cache Memory	Single-bit ECC	32KB		Workstat
Cache Memory	Cache	64KB		Fileserve
Cache Memory	Cache	1,024KB		Fileserve
Cache Memory	Single-bit ECC	3,072KB		Workstat
Cache Memory	Single-bit ECC	256KB		Workstat
Cache Memory	Single-bit ECC	32KB		Workstat
Type: Disk Drive				

Overview of all tracked components.

5.1 Reports

The components of the tracked devices are displayed in reports by category. The available reports are described below.

Report	Description
Software	Overview of applications installed on the devices, including the software version.
Updates	Overview of Windows Updates conducted and when the updates were installed
Hardware	Overview of installed hardware components (including **Type**, **Name**, and **Manufacturer**) This overview contains all the reports listed below.
Processor	Overview of processors installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Motherboard	Overview of motherboards installed in the devices (including **Name**, **Details**, and **Manufacturer**)
BIOS	Overview of BIOS installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Physical Memory	Overview of internal memory installed in the devices (including **Name**, **Details** and **Manufacturer**).
Cache	Overview of caches installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Disk Drive	Overview of hard drives installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Optical Drive	Overview of optical drives installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Logical Disk	Overview of logical disks installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Floppy Disk Drive	Overview of floppy disk drives installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Tape Drive	Overview of optical drives installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Video Controller	Overview of graphics cards installed in the devices (including **Name**, **Details**, and **Manufacturer**)
Active monitor	Overview of monitors connected to the devices (including **Name**, **Details**, and **Manufacturer**)

Report	Description
Network	Overview of network cards installed in 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**)
Sound Device	Overview of the sound cards installed in the devices (including **Name**, **Details**, and **Manufacturer**)

6 Anti-Malware

To protect your devices against malware, use the ITbrain service **ITbrain Anti-Malware**.

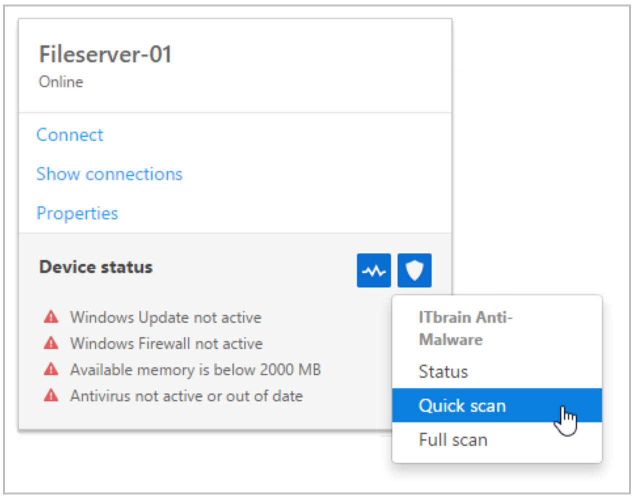
The configured devices (*Section 3.2 "Activating ITbrain for end-points", page 9*) are scanned and protected by the assigned policies defined under *Section 3.3.1 "Configuring policies", page 12*.

Whenever malware is detected on the device, an alert is triggered and displayed as an alert message in the TeamViewer Management Console and the TeamViewer full version. An alert message indicates that malware was detected on one of the devices.

6.1 Manual scans

Start a manual scan for individual end-points. Check the endpoints for malware, regardless of scheduled scans from the Anti-Malware policies, at any time.

A manual scan be started from within the TeamViewer Management Console or the TeamViewer full version for each online device.



Fileserver-01
Online

Windows Update not active
Windows Firewall not active
Available memory is below 2000 MB
Antivirus not active or out of date

Manual scan of an end-point.

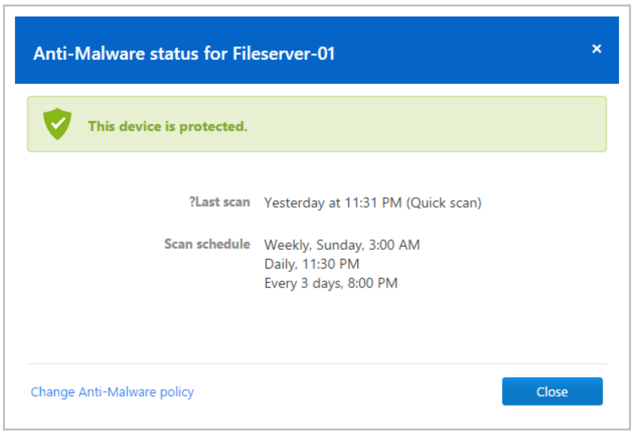
To start a manual Anti-Malware scan, choose one of the following methods:

- In the TeamViewer Management Console, click the name of the end-point and select the 🛡 **| Quick scan** or 🛡 **| Full scan** option.
- In the TeamViewer full version, select the ⚙▾ **| Quick scan** or ⚙▾ **| Full scan** option within the context menu (right click) of the end-point.

6.2 Status of the device

For every end-point, the status of their Anti-Malware scan can be called up. The status contains information about time and date of the previousand next scheduled scans as well as details about the device's protection in general.

- Click on the name of a device and select the 🛡 **| Status** option from the context menu.


Anti-Malware status for Fileserver-01
×
Change Anti-Malware policy
Close

This device is protected.

?Last scan Yesterday at 11:31 PM (Quick scan)

Scan schedule Weekly, Sunday, 3:00 AM
Daily, 11:30 PM
Every 3 days, 8:00 PM

The **Anti-Malware status for** <**DEVICENAME**> dialog box.

The following information is displayed in the **Anti-Malware status for** dialog box:

	Description
Status	The status of the device can be identified by its color. • **Green**: The end-point is protected. • **Yellow**: Minor issue, e.g. old malware definitions or scheduled scan was not performed. • **Red**: Ongoing issue, e.g. malware was found but not removed
Last Scan	Date, time and scan type of the latest scan.
Scans scheduled	All scheduled scans for the end-point as defined in the Anti-Malware policy.

6.3 Alert Report

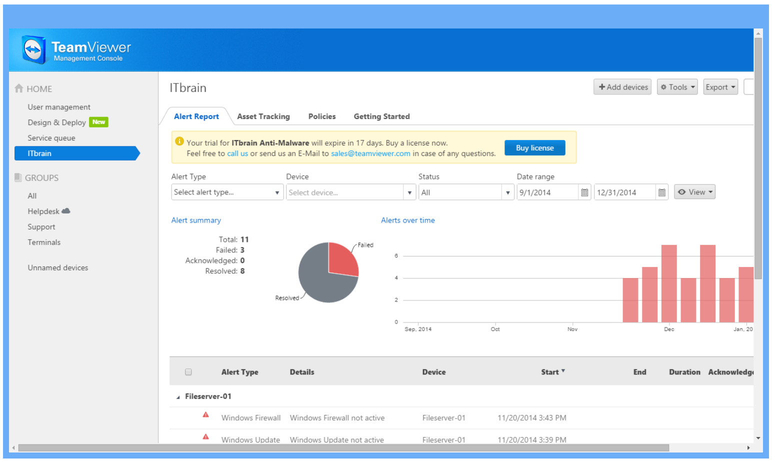
Alert messages for every computer that has ITbrain installed are displayed in the TeamViewer Management Console. An alert message is triggered as soon as irregularities are noticed for a device. This depends on the defined ITbrain policies.

The **Default Anti-Malware policy** includes the following scans, which are described in *Section 3.3.1 "Configuring policies", page 12*:

- Quick scan, daily 09:00 AM
- Full scan, daily at 12:00 PM

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

- In the sidebar, click **ITbrain** and select the **Alert Report** tab. Then select an **alert type**.
- In the sidebar, click on a group from your Computers & Contacts list and select the **Alert Report** tab. Then select an **alert type**.



Your trial for **ITbrain Anti-Malware** will expire in 17 days. Buy a license now.
Feel free to call us or send us an E-Mail to sales@teamviewer.com in case of any questions.

Alert Type: Select alert type...
Device: Select device...
Status: All
Date range: 9/1/2014 – 12/31/2014

Total: **11**
Failed: **3**
Acknowledged: **0**
Resolved: **8**

☐	Alert Type	Details	Device	Start	End	Duration	Acknowledg
Fileserver-01							
⚠	Windows Firewall	Windows Firewall not active	Fileserver-01	11/20/2014 3:43 PM			
⚠	Windows Update	Windows Update not active	Fileserver-01	11/20/2014 3:39 PM			

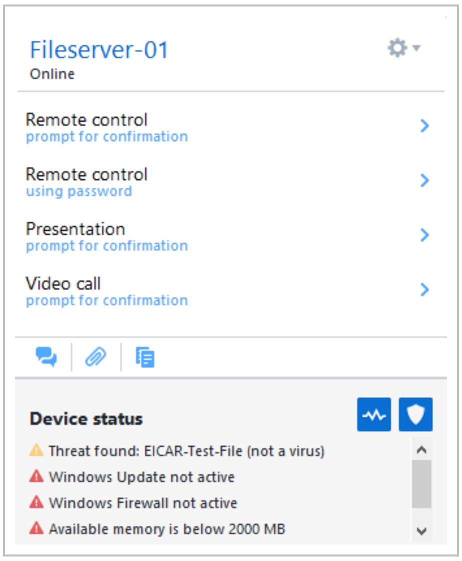
Alert messages are shown in the Alert Report.

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 by the according column. Using the **View** menu, you can define which columns should be displayed for the table and activate or deactivate the charts.

If a threat is detected during a scan, the detected malware will be moved to the quarantine folder immediately. The maleware cannot cause any damage there. In addition, an e-mail notification is sent to the e-mail addresses you have defined for the policy.

The status of the alerts is indicated by different icons.

Icon	Description
⚠	Malware was found on the device. The threat could not be neutralized or moved to quarantine. **Caution**: In this case, please contact the ITbrain Support.
⚠	A threat was found on the device. The threat was neutralized and moved to quarantine.
✓	You have acknowledged the threat. The threat is no longer displayed.



Fileserver-01
Online

Remote control
prompt for confirmation

Remote control
using password

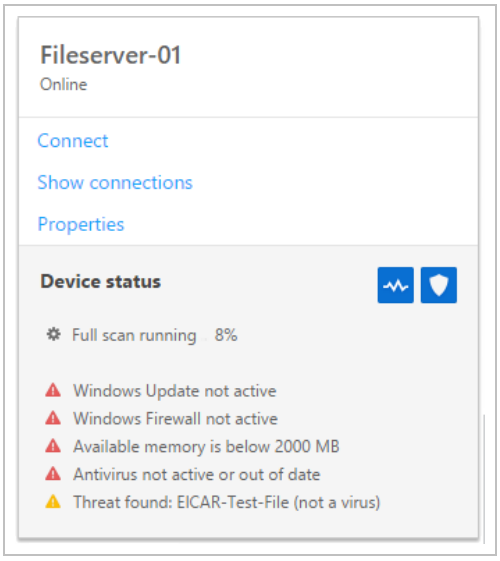
Presentation
prompt for confirmation

Video call
prompt for confirmation

Device status

⚠ Threat found: EICAR-Test-File (not a virus)
⚠ Windows Update not active
⚠ Windows Firewall not active
⚠ Available memory is below 2000 MB

Alert within the Computers & Contacts list caused by malware.



Fileserver-01
Online

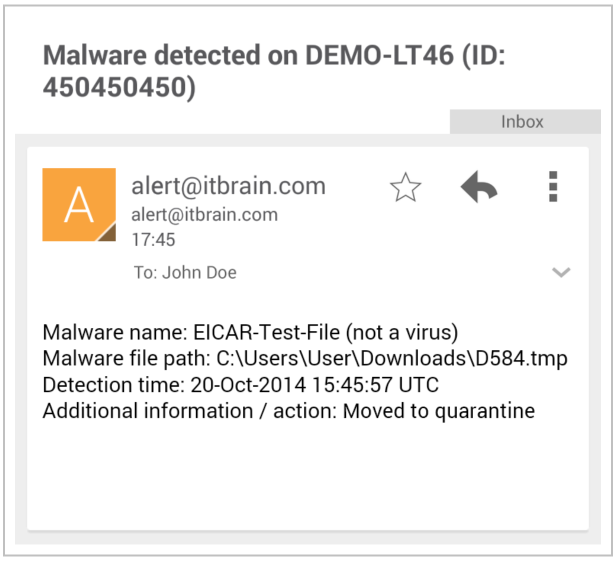
Connect
Show connections
Properties

Device status

Full scan running 8%

⚠ Windows Update not active
⚠ Windows Firewall not active
⚠ Available memory is below 2000 MB
⚠ Antivirus not active or out of date
⚠ Threat found: EICAR-Test-File (not a virus)

Alert message within the TeamViewer Management Console caused by malware.



Malware detected on DEMO-LT46 (ID: 450450450)

alert@itbrain.com
alert@itbrain.com
17:45
To: John Doe

Malware name: EICAR-Test-File (not a virus)
Malware file path: C:\Users\User\Downloads\D584.tmp
Detection time: 20-Oct-2014 15:45:57 UTC
Additional information / action: Moved to quarantine

E-mail notification for malware.

6.4 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 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 email. Verify the notification within the TeamViewer Management Console. Now that you know what the thread 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 the following ways:

- Click the ⚙ ▾ icon next to an alert message and select the **Acknowledge** option.
- Select all the alert messages that you wish to acknowledge and click **Tools | Acknowledge selected.**

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

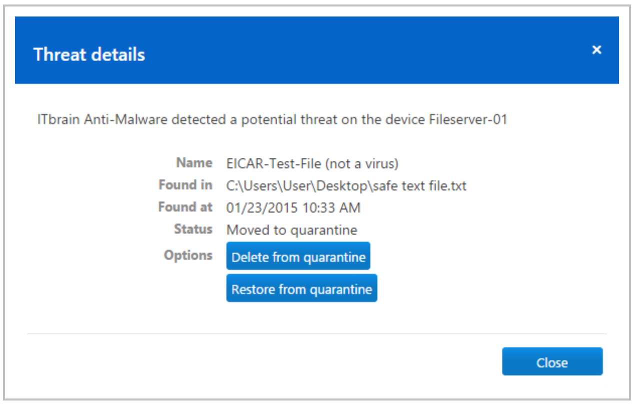
> **Hint**: It is also possible to acknowledge a threat within the Computers & Contacts list (TeamViewer full version and TeamViewer Management Console).

6.5 Threat details

You can display detailed information on detected malware. Get information about the malware type and be better able to rate the threat of the malware.

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

- Click the ⚙ ▾ icon next to an alert message and select the **Details** option.
- Select all the alert messages that you wish to acknowledge and click **Tools | Details**.



Threat details

ITbrain Anti-Malware detected a potential threat on the device Fileserver-01

Name: EICAR-Test-File (not a virus)
Found in: C:\Users\User\Desktop\safe text file.txt
Found at: 01/23/2015 10:33 AM
Status: Moved to quarantine
Options: Delete from quarantine / Restore from quarantine

The **Threat details** dialog.

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

	Description
Device	Name of the device, where the malware was found.
Name	Name of the malware.
Found in	Path or file where the malware was found.
Found at	Date and time when the malware was detected
Options	Select how you would like to proceed with the malware. • **Delete from quarantine**: Click the button if you want to remove the malware from quarantine and permanently delete it. • **Restore from quarantine**: Click the button if you want to restore the malware to its original location and remove it from quarantine. **Caution**: Only restore malware if you are completely sure that the file cannot cause damage to the device.