1 Using CIFS Integrity Monitoring

Document ID: 108419_en_00
Document designation: AH EN MGUARD CIFS

Make sure you always use the latest documentation.
It is available for download at phoenixcontact.net/products.

The use of CIFS IM is subject to licensing and is not available on all devices.

Contents of this document

This document describes how to use the *CIFS Integrity Monitoring* mGuard function.

1.1 Introduction

CIFS stands for *Common Internet File System*, better known as *Windows File Sharing*.

CIFS Integrity Monitoring (CIFS-IM) is antivirus protection – or an antivirus sensor – for use in industrial applications that is able to detect whether a Windows-based system (machine controller, operator interface, PC) has been infected with malicious software, without the need to load virus signatures.

As a part of the CIFS integrity check, the Windows shares are checked to determine whether certain files (e.g. *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

CIFS-IM can also be used for version control and monitoring.

1.1.1 Purpose

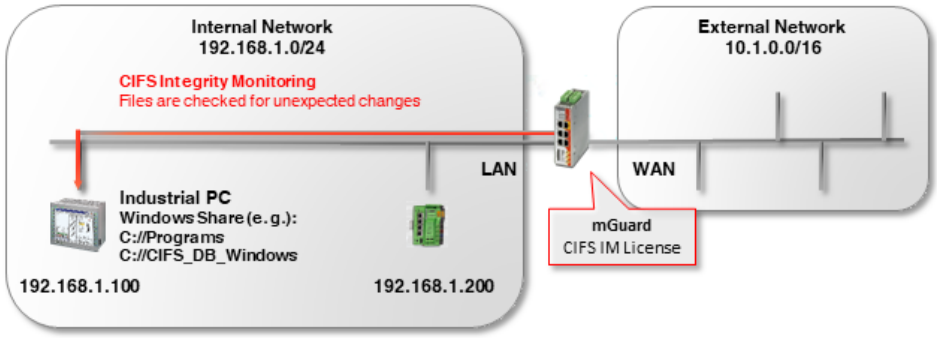

Figure 1-1 CIFS Integrity Monitoring – diagram

CIFS-IM is generally used in conjunction with the firewall function on mGuard devices for protecting *non-patchable systems*.

Non-patchable systems are primarily Window-based systems which either

a) **have an outdated operating system** for which security updates are no longer being provided (e.g. Windows 2000 / Windows XP),

b) **may no longer be modified** because the delivery state has been certified by the manufacturer or an authority and the manufacturer's warranty or the authority's approval would be forfeited in the event of a software modification,

c) **cannot be equipped with a virus scanner**, e.g. due to time-critical industrial applications (*real-time* capacity); or there is no way to update a virus signature because there is no connection to the Internet.

Non-patchable systems can be found in a number of different branches of industry. These include medicine (e.g. MRI, CT), the chemical and pharmaceutical industry (e.g. analysis systems), but also in production (e.g. PC-based machine controllers, plant data collection).

1.1.2 Method of operation

As a part of the **CIFS integrity check**, Windows shares are regularly checked to determine whether certain (executable) files (e.g. *.exe, *.dll) have been changed compared to a reference status in the integrity database.

The **integrity database** contains the checksums (hash values) for all the files that are checked. If the checksum of a file has changed, this indicates that the file has been modified, which in turn indicates a possible virus/worm attack or unauthorized intervention. It also detects whether new files have been added or files have been deleted.

The integrity database is created either when a share is checked for the first time or upon explicit request (e.g. after intentionally changing one or more files on the share). It is signed with an mGuard device machine certificate which protects it against tampering.

If the CIFS integrity check detects a deviation, an alarm can be sent out via e-mail or SNMP (SNMP trap).

1.1.3 Advantages over other antivirus systems

CIFS Integrity Monitoring offers the following advantages in the industrial environment:

a) There is no or almost no burden on the system being monitored (CPU performance, network load).
b) A connection to the Internet or to an update server is not required.
c) There is no need to reinstall virus signatures.
d) There are generally no false alarms (*false positives*) – and if one does occur, it has no effect on the system being monitored, since no data is deleted or moved to quarantine.

1.2 Configuration Example

On a Windows PC, the directory that is monitored is *C://Programs*. A user with the user name *CIFS* is created on the PC being monitored who has read access to the *C://Programs* directory.

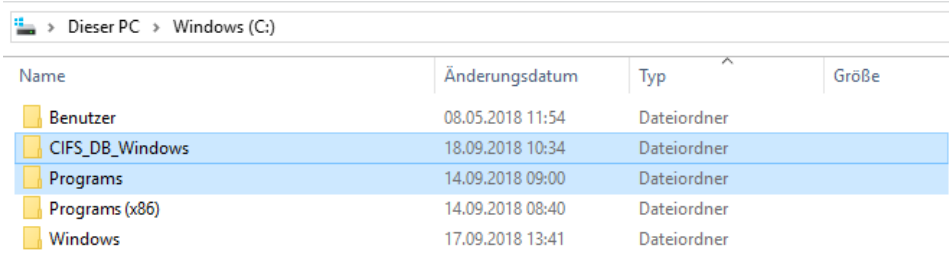

Figure 1-2 Creating directories / the integrity database

The integrity database should be saved to the *CIFS_DB_Windows* directory on the PC being monitored. The *CIFS* user also has read/write access to this directory.

1.3 Requirements

– The PC to be monitored must be situated in the network 192.168.1.0/24 and be accessible at the IP address 192.168.1.100.
– The mGuard device must be accessible at the IP address 192.168.1.1.
– The optional *CIFS Integrity Monitoring* license is present and available for purchase on the device.

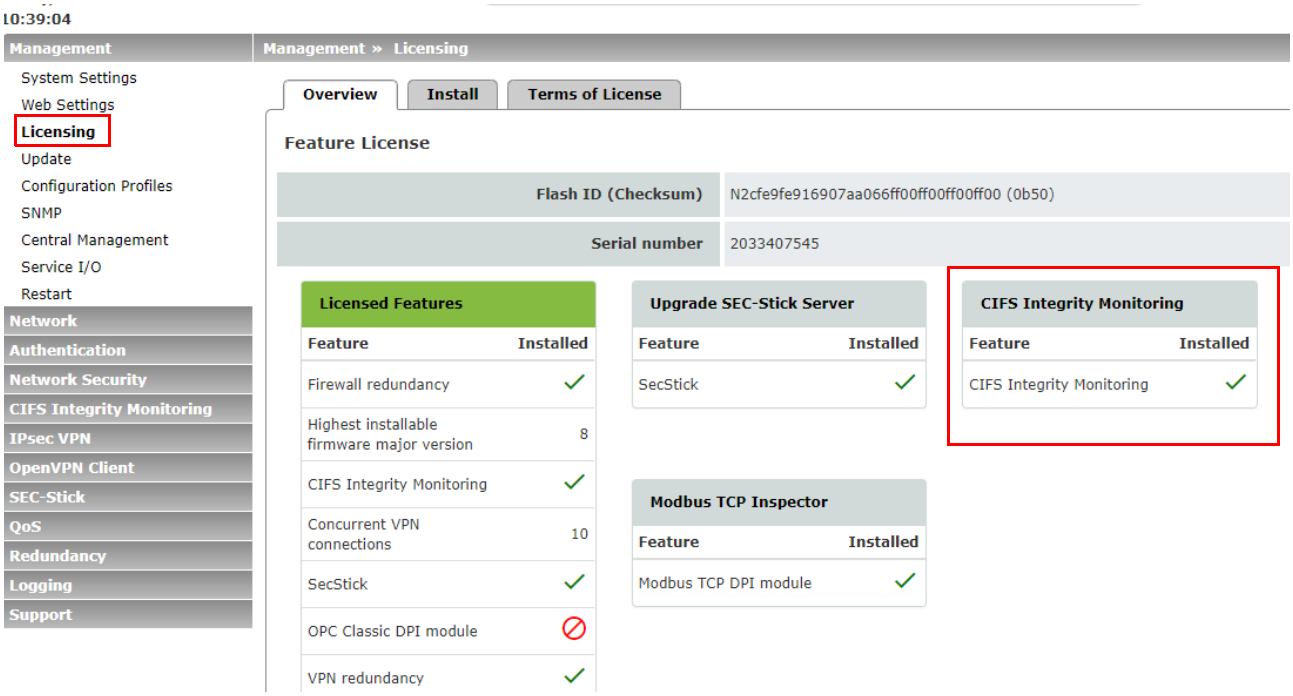

Figure 1-3 CIFS Integrity Monitoring license on the device

CIFS-IM is configured using the web-based management tool on the mGuard device (shown here: firmware version 8.7.0).

1.4 Importing a machine certificate

The machine certificate selected in the CIFS IM menu as the *integrity certificate* is used to sign and check the integrity database so that it cannot be replaced or tampered with by an intruder without being detected.

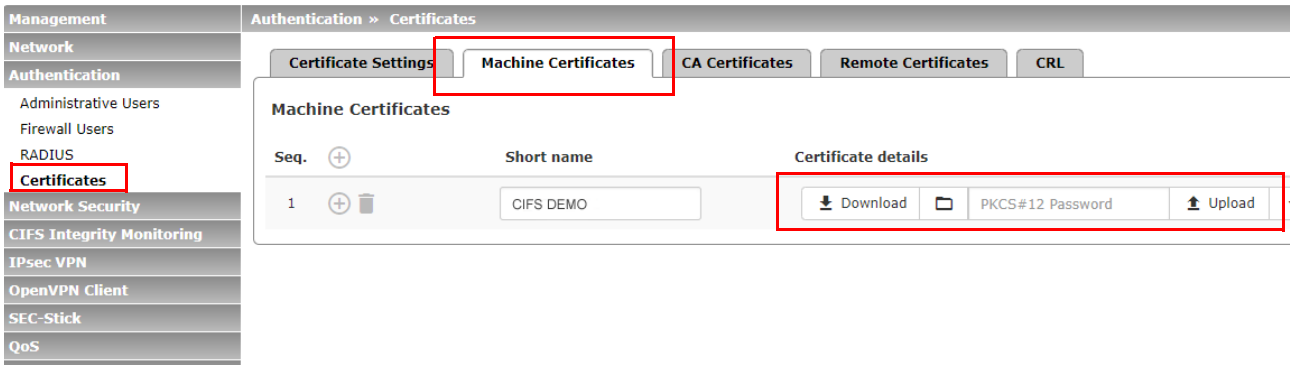

Figure 1-4 Installed machine certificate for use with CIFS IM

To import a machine certificate, proceed as follows:

1. Log on to the mGuard device web-based management.
2. Go to **Authentication >> Certificates** (*Machine certificates* tab).
3. Click on the ⊕ icon to add a new machine certificate.
4. Click on the 🗀 icon to select the certificate file (PKCS#12) on the installation computer.
5. Enter the PKCS#12 password issued when generating the certificate.
6. Give the certificate a unique short name. If you leave this field empty, the *common name (CN)* of the certificate is used automatically.
7. Click on the **Upload** button to import the certificate into the mGuard device.
8. Click on the "*Save*" icon 💾 to complete the import.

1.5 Configuring/importing shares

The Windows shares to be monitored are configured or imported on the mGuard device. The location where the integrity database and the test report should be stored is also configured/imported as a share.

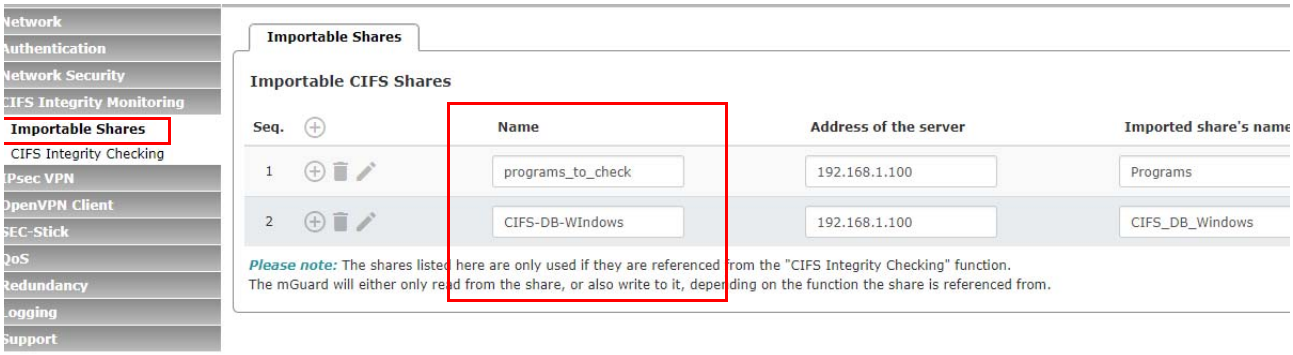

Figure 1-5 Imported shares for use with CIFS-IM

To import shares into the mGuard device, proceed as follows:

- Go to **CIFS Integrity Monitoring >> Importable Shares**.
- Click on the ⊕ icon to add a new share.
- Click on the ✎ icon to configure the share.

The designations that the mGuard device uses to internally manage the shares is indicated under **Name**. **Imported share's name** is the name of the approved Windows directory and must be adopted exactly as is:

  - The **name** *"programs_to_check"* is the internal mGuard designation for the **Imported share's name** *"C:\Programs"*.
  - The **name** *"CIFS- DB-Windows"* is the internal mGuard designation for the **Imported share's name** *"C:\CIFS_DB_Windows"*.

⇒ The mGuard device now knows the shares and can check them.

1.6 Configuring parameters for integrity checks

The integrity certificate used to sign the integrity databases must now be selected. If you wish to receive e-mail notification of integrity checks when they are done, you must configure the settings here accordingly.

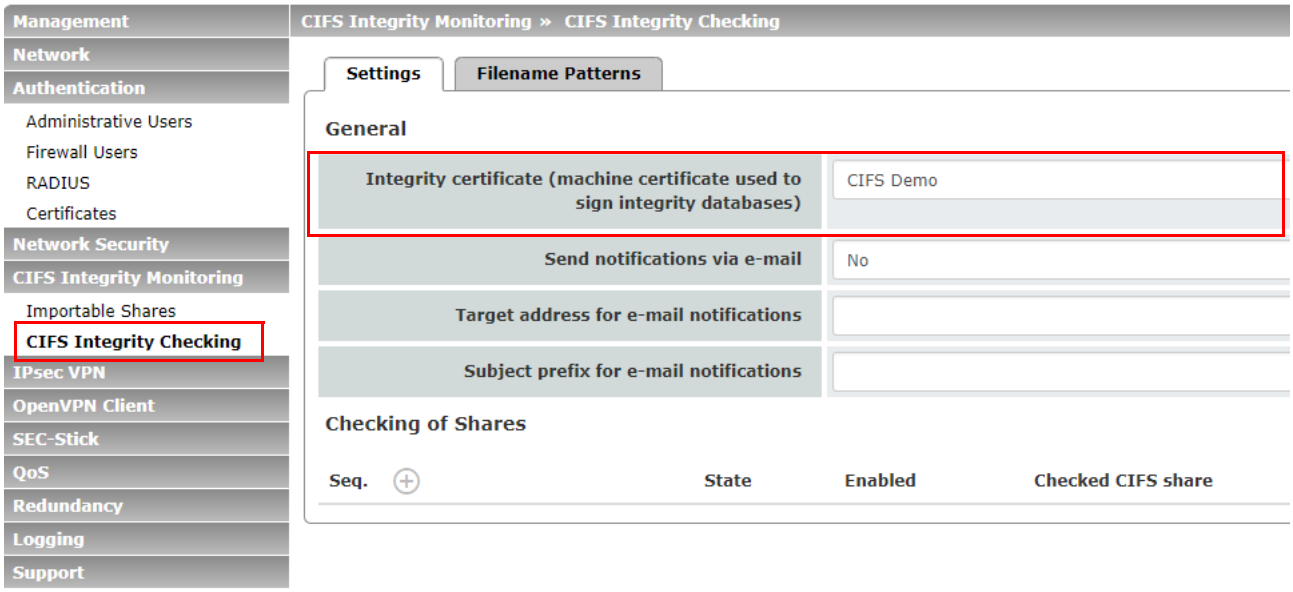

Figure 1-6 Selecting the machine certificate and configuring e-mail notification

- Go to **CIFS Integrity Monitoring >> CIFS Integrity Check** (*Settings tab*).
- Select the machine certificate to be used for the CIFS IM.
- **Optional**: Specify whether an e-mail notification should be sent (with every integrity check or only if errors/deviations are found).
  The mGuard device must have access to an e-mail server for this option. Configure this under **Management >> System Settings** (*E-Mail* tab).

1.7 Specifying the files to check

The file types and/or file directories to be included or excluded from monitoring are specified on the *Filename Patterns* tab.

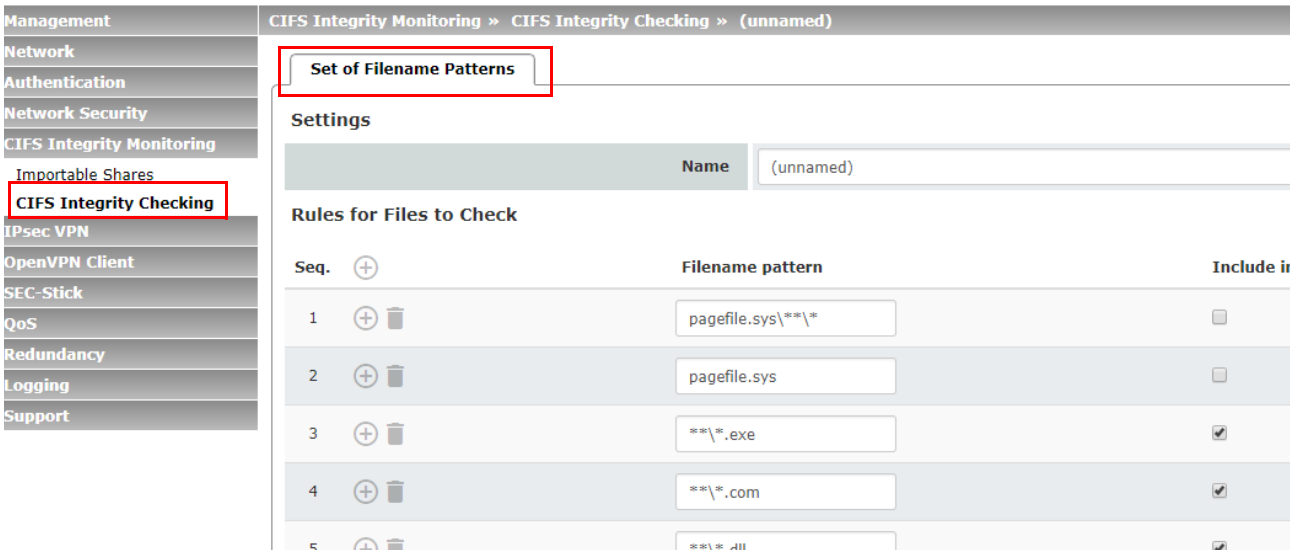

Figure 1-7 The files to be checked are specified using patterns

Proceed as follows:

- Go to **CIFS Integrity Monitoring >> CIFS Integrity Checking** (*Filename Patterns* tab).
- Specify the file types or file patterns to be checked.
  The mGuard device starts by offering a file pattern that can be either adopted or modified.

Patterns for filenames

***.exe means that the files located in a specific directory and with file extension **.exe* are checked (or excluded).

** at the start means that any directory is searched, even those at the top level, if this is empty. This cannot be combined with other characters (e.g., *c*** is not permitted).

Placeholders (*) represent any characters, e.g. *win**.exe* returns files with the extension **.exe* that are located in a directory that begins with *win*... Only one placeholder is permitted per directory or file name.

Example: *Name***.exe* refers to all files with the extension *.exe* that are located in the "*Name*" directory and any subdirectories.

Include in check

Activate function (include): files are included in the check.
Deactivate function (exclude): files are excluded from the check.

(Each file name is compared with the patterns in sequence. The first hit determines whether the file is to be included in the integrity check. The file is not included if no hits are found.)

1.8 Creating check sequences

You can create one or more check sequences that check different shares, directories, or file types.

A time-controlled check is configured for each check sequence (see also the mGuard firmware manual, available at phoenixcontact.net/products or help.mguard.com).

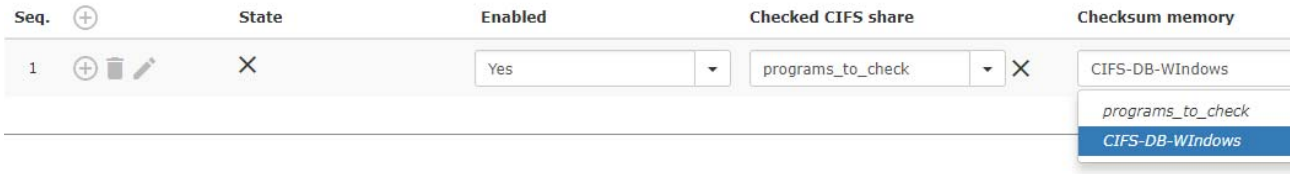

Figure 1-8 Creating a check sequence and selecting shares

Proceed as follows to create and configure a check sequence:

- Go to **CIFS Integrity Monitoring >> CIFS Integrity Check** (*Settings tab*).
- **Checking of Shares** section: Click on the ⊕ icon to create a new check sequence.
- Select the share to be checked from the drop-down list.
- Select the share to be used as the checksum memory from the drop-down list.
- Click on the ✎ icon to configure the parameters for a check sequence.

The parameters are all preset to defaults on the *Checked Share* tab. If need be, however, you can make changes here.

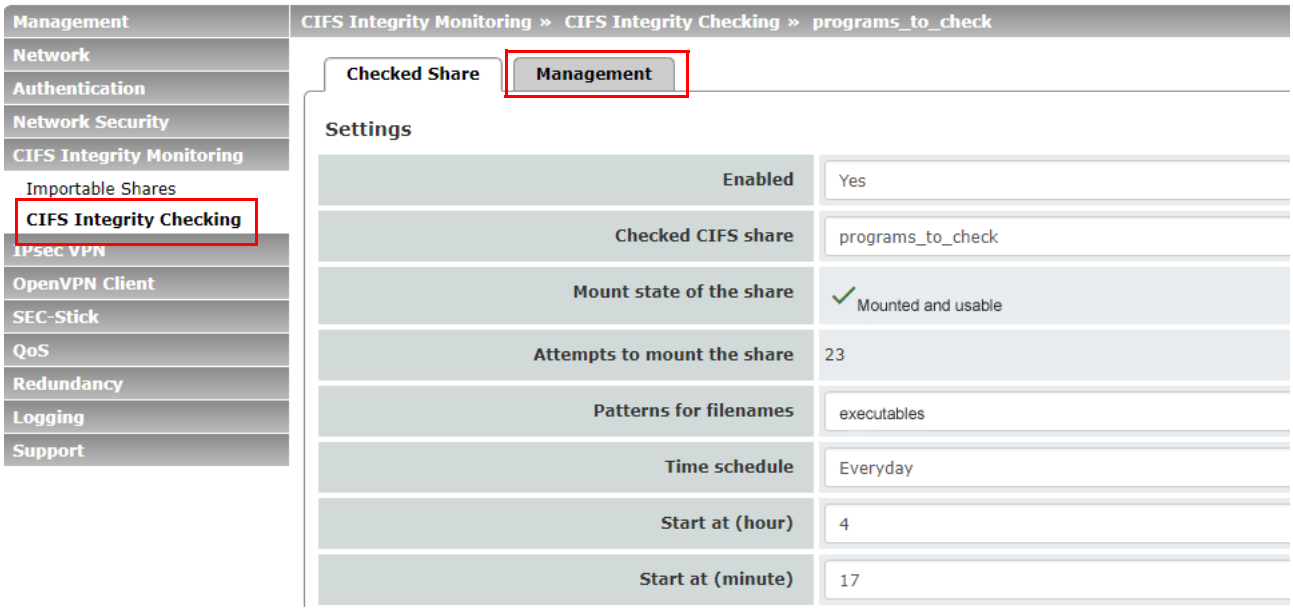

Figure 1-9 Parameter settings for checking the share

1.9 Initializing the integrity database

If a share to be checked is reconfigured, a corresponding integrity database must be created. This integrity database is used as the basis for comparison when checking the share regularly. It stores the checksums for all of the files to be monitored. The integrity database itself is signed with the integrity certificate to protect it against manipulation.

The integrity database is initialized on the *Management* tab.

First run a check to determine whether the mGuard device has read access to all of the files and directories on the monitored share (*Start an access check*).

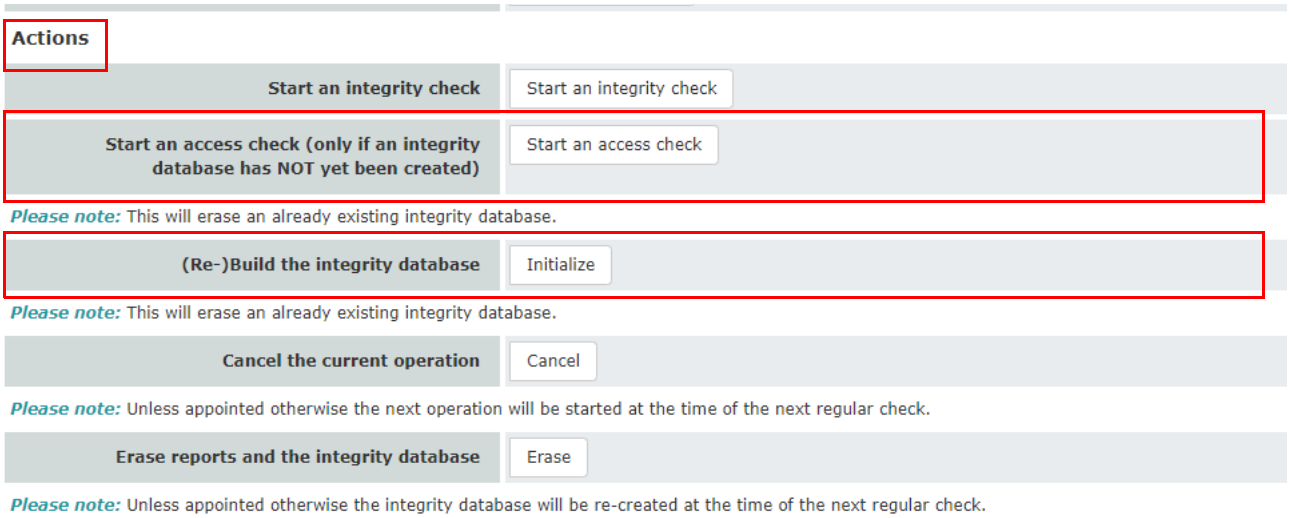

Figure 1-10 Preparing and starting an integrity check

Proceed as follows to (re)initialize the integrity database:

- Go to **CIFS Integrity Monitoring >> CIFS Integrity Check** (*Settings tab*).
- In the **Checking of Shares** section, click on the icon to configure check sequence parameters.
- The parameters are all preset to defaults on the *Checked Share* tab. If need be, you can make changes here.
- Switch to the *Management* tab.
- Click the **Start an access check** button (see Table 1-1).

⇒ The system checks to determine whether the access privileges required for the check are in place.

- If the privileges are in place, click on the **Initialize** button (see Table 1-1).

⇒ The integrity database is created and then used as a reference for further checks.

1.10 Options for actions when creating an integrity database

The actions that you can carry out as part of the CIFS Integrity Monitoring are briefly described in Table 1-1.

For a precise description, see also the mGuard firmware manual, available at phoenixcontact.net/products or help.mguard.com.

Table 1-1 Preparing and starting an integrity check – description of functions

Function name	Description
Start an integrity check	Clicking on the *Start an integrity check* button starts the integrity check. The result of the check can be viewed in the report by clicking on the *Download report* button.
Start an access check **(only if an integrity database has NOT yet been created)**	**NOTE: Any existing integrity database will be deleted.** Click on the *Start an access check* button to check whether there are files present on the imported share that the mGuard device cannot access. This prevents a more comprehensive creation of the integrity database from being aborted due to lack of the proper access permissions. The result of the check can be viewed in the report by clicking on the *Download report* button.
(Re-)Build the integrity database	**NOTE: Any existing integrity database will be deleted.** The mGuard device creates a database with checksums so that it can determine later whether files have been changed. A change to executable files indicates a virus. If files have been changed, rebuilt, or deleted intentionally, a new database must be created by clicking on the *Initialize* button in order to prevent false alarms. The creation of an integrity database is also recommended if shares have been newly set up. Otherwise, an integrity database is set up during the first scheduled check instead of a check being performed (if an access check was not performed first).
Cancel the current operation	Click on the Cancel button to stop the integrity check.
Erase reports and the integrity database	**NOTE: Any existing integrity database will be deleted.** Click on the *Erase* button to delete all existing reports/databases. A new integrity database must be created/initialized for any further integrity checks. This can be initiated by clicking on the *Initialize* button. Otherwise, a new integrity database is generated automatically at the next scheduled check (if an access check was not performed first). This procedure is not visible.

1.11 Access check performed successfully

If the access check was performed successfully, the following message displays (see Figure 1-11).

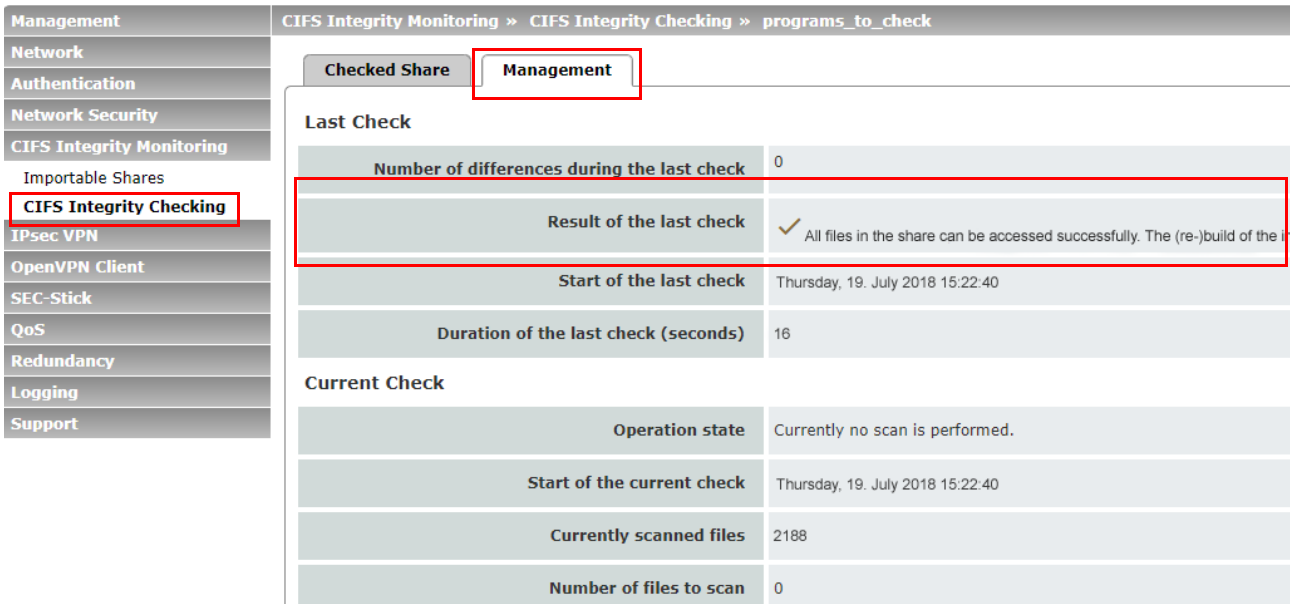

Figure 1-11 Access check successful

⇒ Once an access check has been successfully run, the integrity database can be (re)generated using the "*Initialize*" button under "*(Re-)Build the integrity database*".

1.12 Integrity database build successful

If the integrity database build was successful, the following image is displayed (see Figure 1-12).

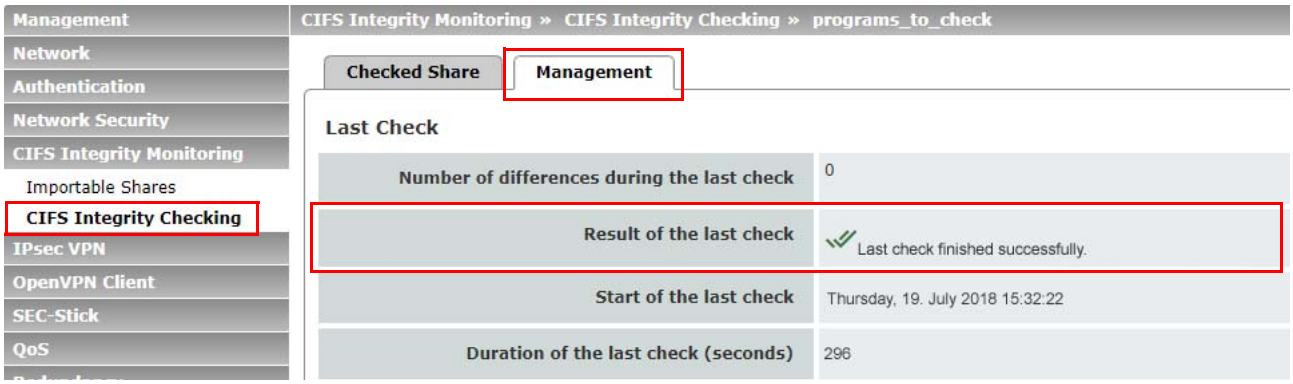

Figure 1-12 Successfully built integrity database

⇒ The integrity database has now been created. The consistency check is then done manually or automatically, depending on the configured time interval.

1.13 Missing access rights (read/write privileges)

If the mGuard device is denied access to any files/directories, the following error message appears.

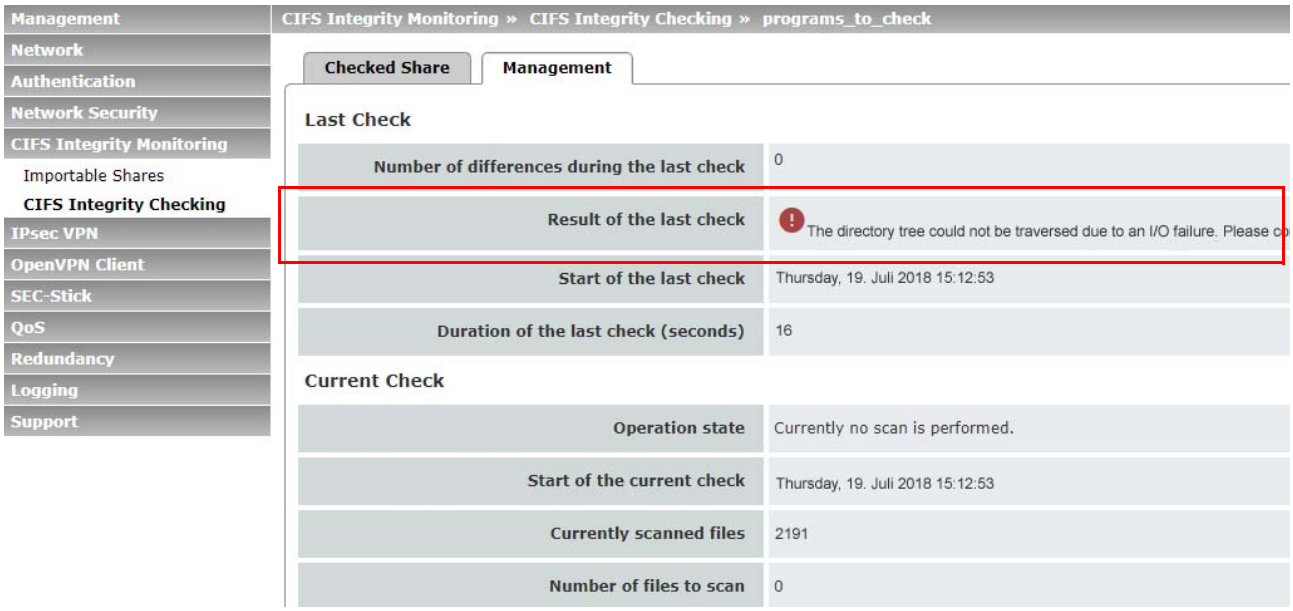

Figure 1-13 Access to files/directories failed

The directories or files in question are listed in the check report. This report is located on the checked PC and can be downloaded there or via the mGuard device's web-based management.

Example:

```
/var/cic/mnt/MAIv042835620-memory/integrity-check-log.txt
START_OF_LOG 2aa83b0b-6484-1787-a2d9-000cbe040098 Thu Jul 19
15:12:53 2018
SUBJECT check-access name=zu-pruefende-Programme
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Permission
denied" path=Gemeinsame Dateien type=d
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Permission
denied" path=Windows NT/ZubehÃ¶r type=d
ACCESS_CHECK_FAILED
END_OF_LOG
```

Figure 1-14 Example: Entry in report for failed read rights

In this case, Windows prevents access to the following directories:

– *Common Files*
– *Windows NT/Accessories*

1.14 Excluding files and directories from the check

If access to one of more files/directories is not possible, they can be excluded from the check.

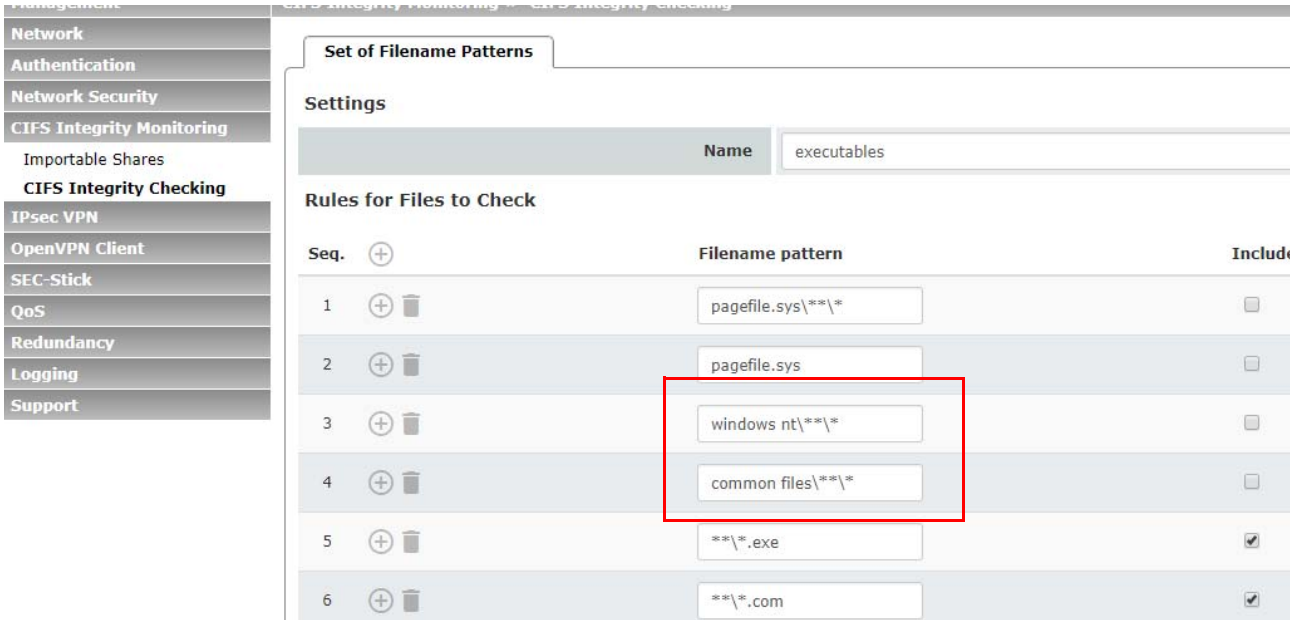

Figure 1-15 Excluding directories from the check

See also Section 1.7, “Specifying the files to check”

Directories that need to be excluded must be inserted in the table in a position before the first ***.

1.15 Performing a CIFS integrity check

Once the integrity database has been successfully created, an integrity check can be performed. This can either be done

– manually via the web-based management or
– via scheduling (see Section 1.8, “Creating check sequences”).

For a description of all of the configuration parameters, see the mGuard firmware manual available at phoenixcontact.net/products or help.mguard.com.

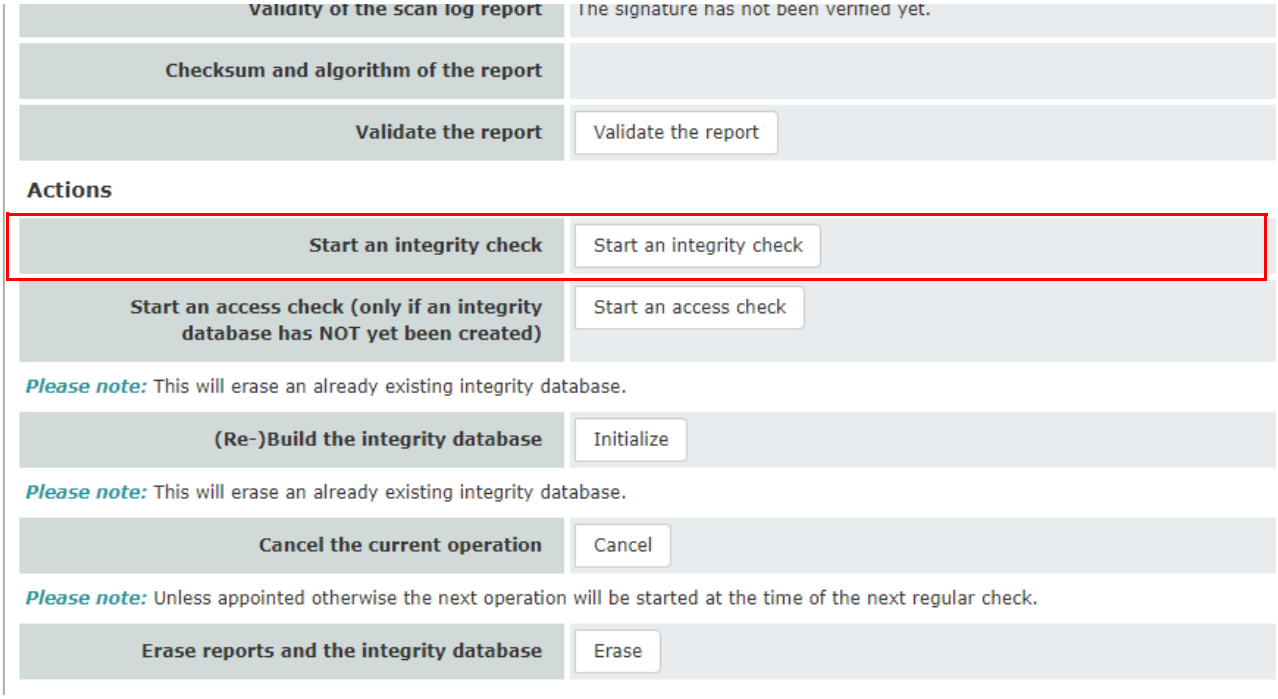

Figure 1-16 Performing an integrity check

Procedure

- Go to **CIFS Integrity Monitoring >> CIFS Integrity Check** (*Settings tab*).
- In the **Checking of Shares** section, click on the icon to configure check sequence parameters.
- The parameters are all preset to defaults on the *Checked Share* tab. If need be, you can make changes here.
- Switch to the *Management* tab.
- Click on the **Start an integrity check** button (see Table 1-1).

⇒ The result of the current check is displayed in the **Current Check** section. A check report is generated.

- Click on the **Validate the report** button to verify the integrity of the check report.
- Click on the **Download report** button to download and analyze the check report.