Outpost24

Vulnerability Management made easy

Compliance Scanning

Quick Start Guide

Version: 2.0

2018-01-18

Table of Contents

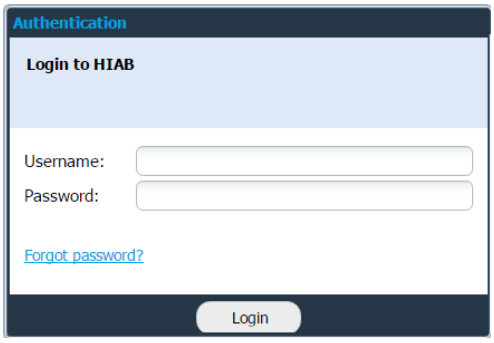
About This Document

This document is meant to provide users with a comprehensive overview of the Compliance Scanning module for HIAB and OUTSCAN. This document has been elaborated under the assumption the reader has access to the HIAB or OUTSCAN Account, and Portal Interface.

For support information, visit https://www.outpost24.com/support.

1 Getting Started

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
Users who have HIAB, connect to your HIAB by using its assigned network address.
***Note**: Use HTTPS protocol, since the HIAB doesn't have anything listening on HTTP.*



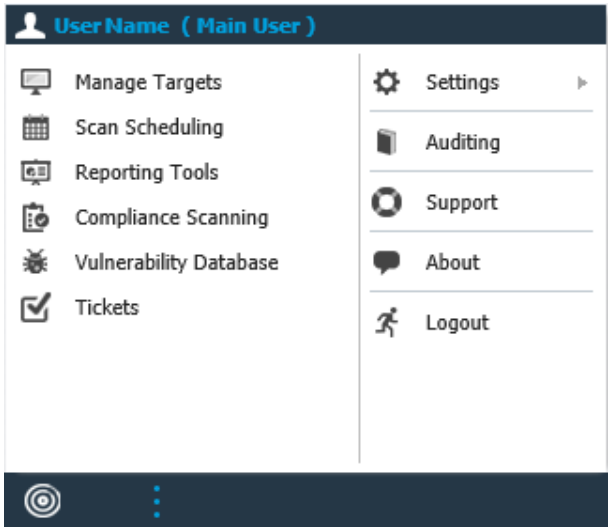
Please log on using your credentials.

To access the Compliance Scanning module, go to
Menu → Compliance Scanning
or
Menu → Target Scanning → Compliance Scanning

2 The Compliance Scanning Interface

The Compliance Scanning Module shows the compliance status of the results from a scan, and export the status to various formats.

Scans can be started by selecting a **Main Menu → Scan Schedule**, or by selecting a target group and then select individual targets in **Main Menu → Manage Targets**.



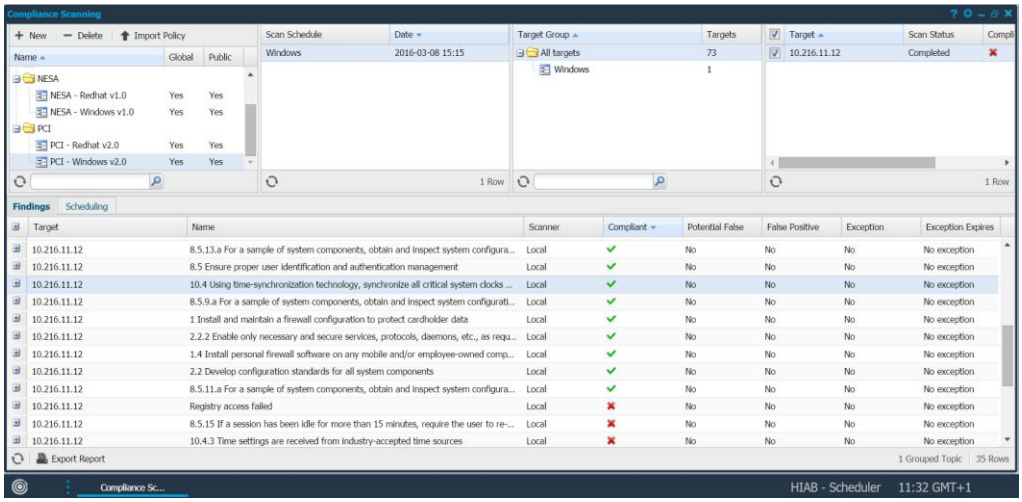
2.1 Interface Sections

The interface consists of two sections:

- Top section
- Lower section

In the Top section, targets can be selected for scanning. For each scan of a target, a compliance report is created.
For more information see *2.2*

Interface Top Section.

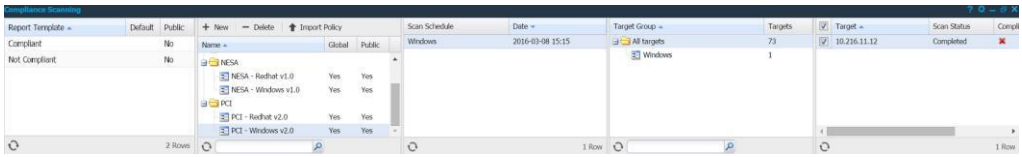


***Note**: The Compliance Scanning will only show the scans from Scan Schedules which had Compliance Scanning enabled under the Scan Settings tab.*

The Lower section lists all the targets that were found based on the selection in the top area. For more information see *2.3 Interface Lower Section*.

2.2 Interface Top Section

The Top Section determines what you will see in the compliance report.



2.2.1 Report Template

The Report Template grid is not visible the first time you access the Compliance module. This grid is displayed first when a Report Template have been saved, which is done by filtering the lower section and save those filtering options.
See section *2.3.1 Technical Tab* for more information on displaying findings.

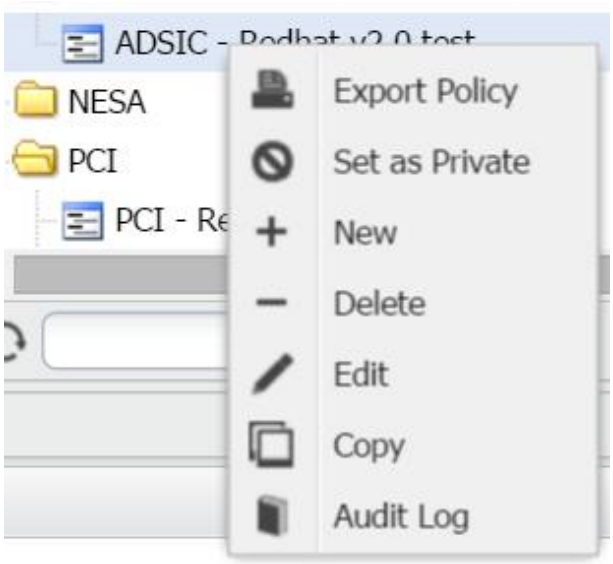
2.2.2 Compliance Policy

The top left section is used to select a compliance policy. A policy is a predefined set of rules, which includes multiple or singular requirements that defines the compliance policy and reports based on these.

The following are some examples of the pre-defined standards within the Compliance Module:

- ADSIC
- CIS
- GDPR
- HIPAA
- NESA
- PCI

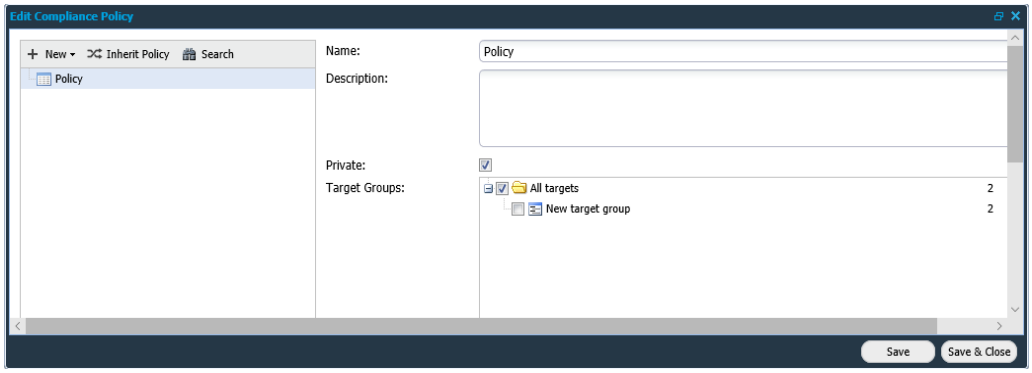
By right clicking any custom defined policy, the following options are presented:



Option	Description
Export Policy	Export the selected policy, this will save the policy locally as an .xml file.
Set as Private	Set the policy as private; the policy will not be visible for any other user within the system.
New	Create a new policy.
Delete	Delete the selected policy.
Edit	Edit the selected policy.
Copy	Create a copy of the selected policy.
Audit Log	View the audit log for the selected policy.

Create New Policy Tab

To create a custom compliancy policy, click **New** to open the *Edit Compliance*.

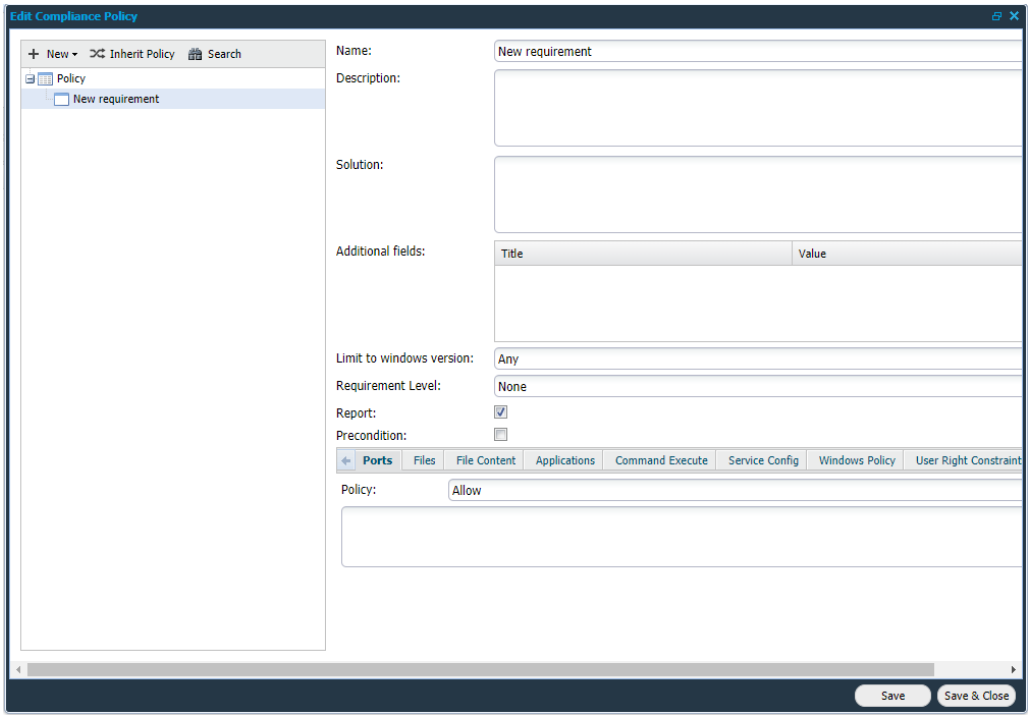


The following attributes are configurable:

Option	Description
Name	Name of the policy.
Description	Enter a description for the policy.
Private	Defines if the policy should be private or public.
Target Groups	Select target groups.

Create New Requirement Tab

On the left-hand side of the window is the Requirements Tree.



Click **New → Requirement** to create a new requirement, in which the following functionality can be configured for your policy:

Option	Description
Name	Name of the requirement.
Description	Enter a description for the requirement.
Solution	Enter a solution for the requirement.
Additional fields	Right click and choose New to create additional fields to the requirement, these will be shown whenever you expand the requirement in the report.
Limit to windows version	Limit the requirement to a specific Windows version.
Report	By unchecking, this specific requirement will not be reported in the compliance report.
Precondition	Checks if parent requirement is met before evaluation the child requirment.

Add section which makes it clear that the first section of tabs is associated with Linux systems and the later part is associated with Windows controls.

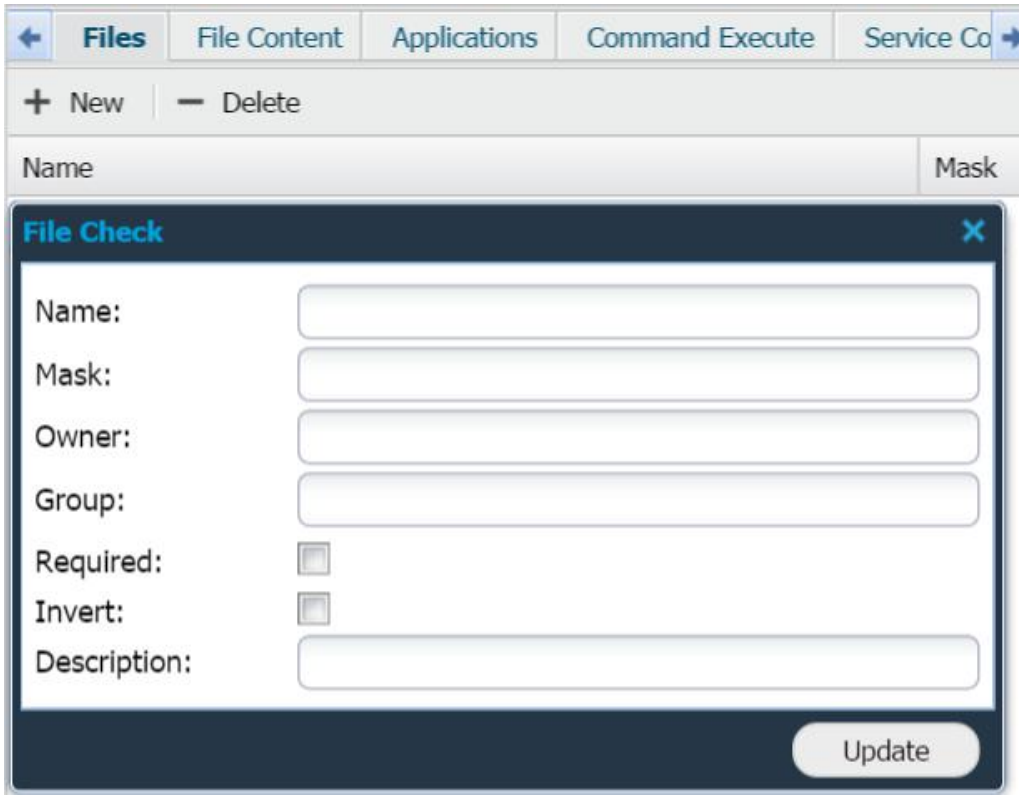
Port Tab

The **Port** tab defines what ports are allowed or disallowed.
Choose from:

- Disallow
- Allow
- Exactly

Files Tab

The **Files** tab defines which files to be allowed or disallowed.
***Note**: Only applicable in Linux.*



Option	Description
Name	Absolute path of the file.
Mask	File permission mask. Enter the octal value of file permissions For example, `640`.
Owner	Owner of the file.
Groups	Group name of the file owner.
Required	Enforce to check the file presence at the given path. The test will fail if the file does not exist at the given path.
Invert	Invert the whole test.
Description	Description for the check.

Mask

Mask consists of octal representation of the expected file permissions.

The scanner interprets the value added and checks for combinations of that value.

Ex.

File permissions are constructed by combinations of

- Read (4)
- Write (2)
- Execute (1)

and each position represent either the *user(owner)*, *group,* or *other (all other users).*

If the file has the permission 640 it means that the file has *read(4) + write(2)* for the user, and *read(4)* for the group, and no permissions (0) for all other.

The scanner checks each position, first 6 then 4 and then 0.

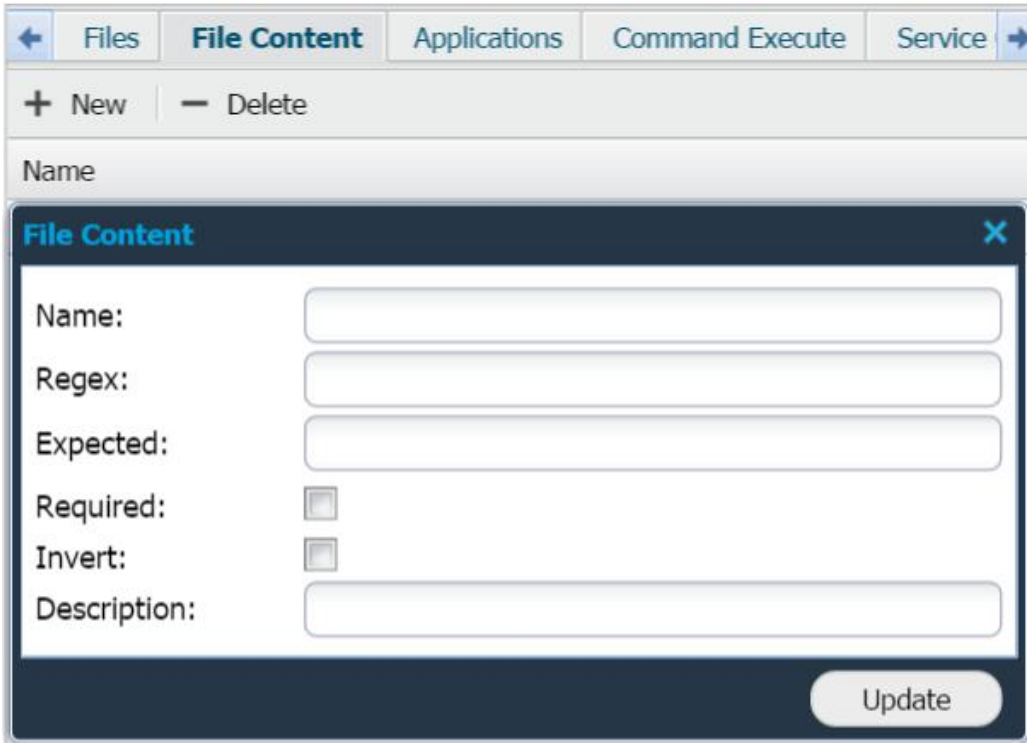
The value 6 (Read+ Write) is created by combining 4 (read) and 2 (write). So, the possible combinations are 6, 4, and 2 (read+write, read, and write).
The scanner checks for any of these permission on the file and returns a positive if found.

If the file has the permission set as 740 read+write+execute for the user, the scanner would return a negative, since execute=1 is not part of the expected combinations.

File Content Tab

The **File Content** tab defines which content that should be allowed or disallowed within a file.

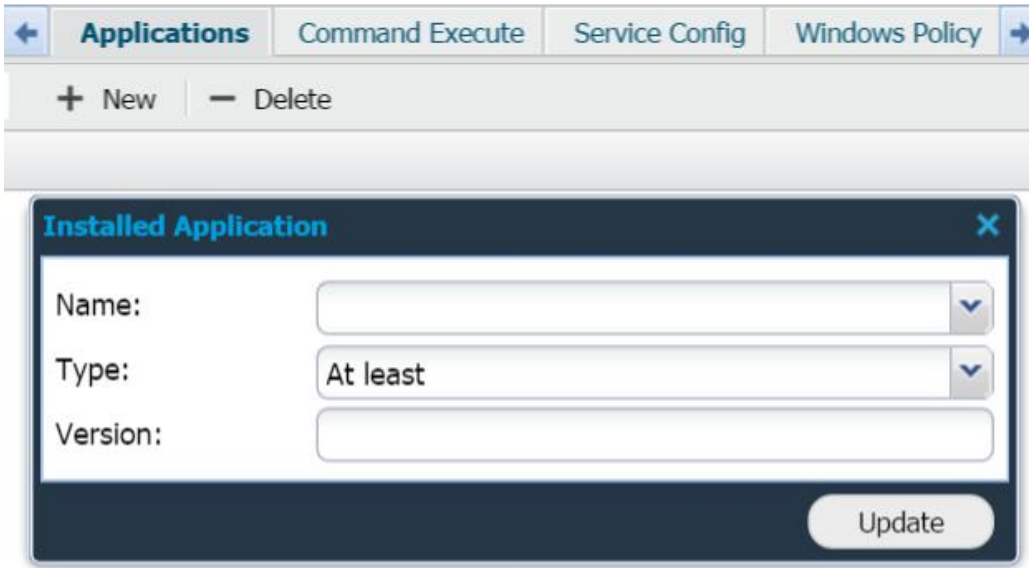
***Note**: Only applicable in Linux.*



Option	Description
Name	Absolute path of the file.
Regex	POSIX extended regular expression to select set of lines. Example: `'^user =*'` gives lines starting with `'user='` ***Note**: expressions are case sensitive.*
Expected	POSIX extended regular expression for what is expected to be present in the selected set of lines. ***Note**: expressions are case sensitive.*
Required	Enforce to check the file presence at the given path. The test will fail if the file does not exist at the given path.
Invert	Invert the whole test.
Description	Description for the check.

Applications Tab

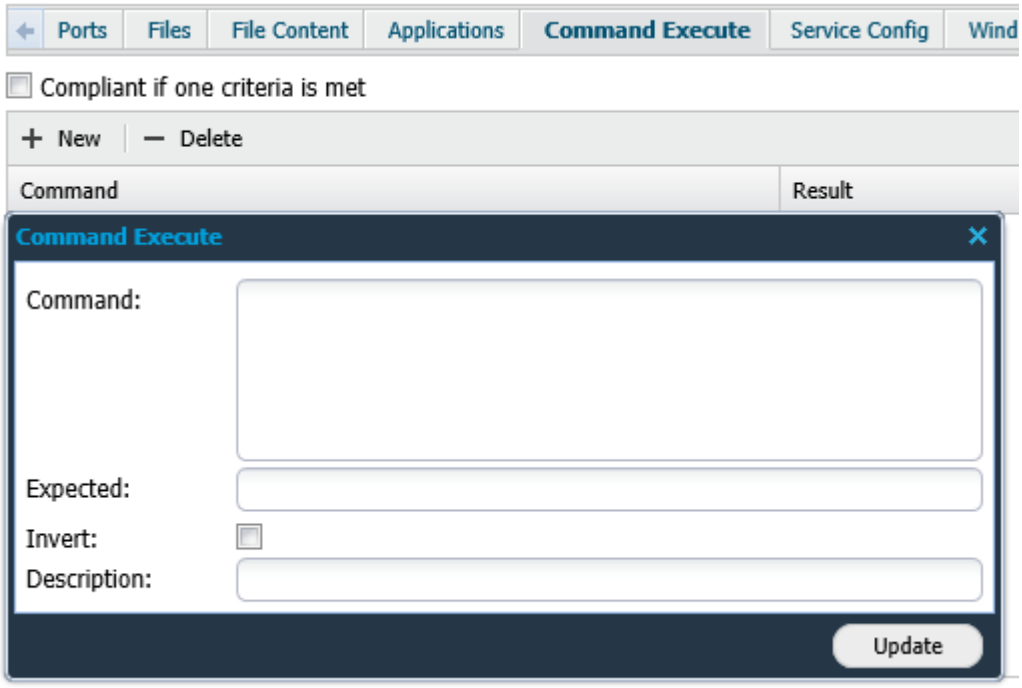
The **Applications** tab define what applications that are allowed or disallowed. It is also possible to define the version of the application



Option	Description
Name	Name of the application.
Type	When comparing with the version number of the application, choose between: ► This ► At least ► At least allow missing ► Not Installed
Version	Version of the application.

Command Execute Tab

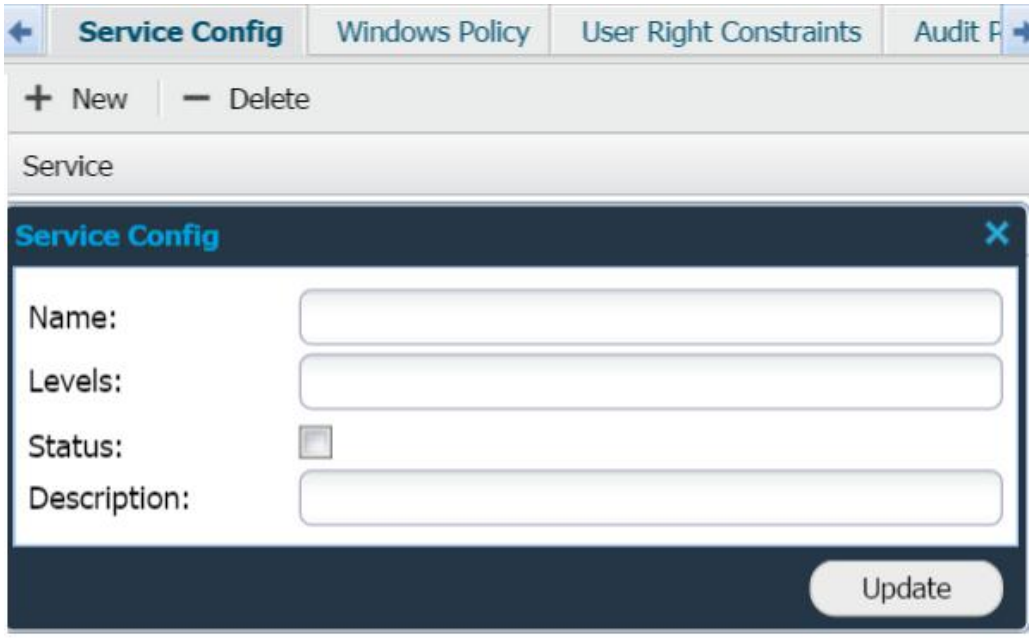
The **Command Execute** tab defines a Linux command to be executed on the target. When there are several commands, checking the '*Compliant if one criteria is met'* stops further execution of remaining commands if one of them delivers a positive result. Executes all commands if 'C*ompliance if one criteria is met*' is left unchecked.



Option	Description
Command	Defines the Linux command. ***Note:*** *The command may be prefixed with "sudo" escalation and need to be written supporting such style. In other words, pipes with greps will then be running with lower privileges.*
Expected	Regular expression for what is expected to be presented in the output of the given command.
Invert	Invert the test.
Description	Description of the check.

Service Config Tab

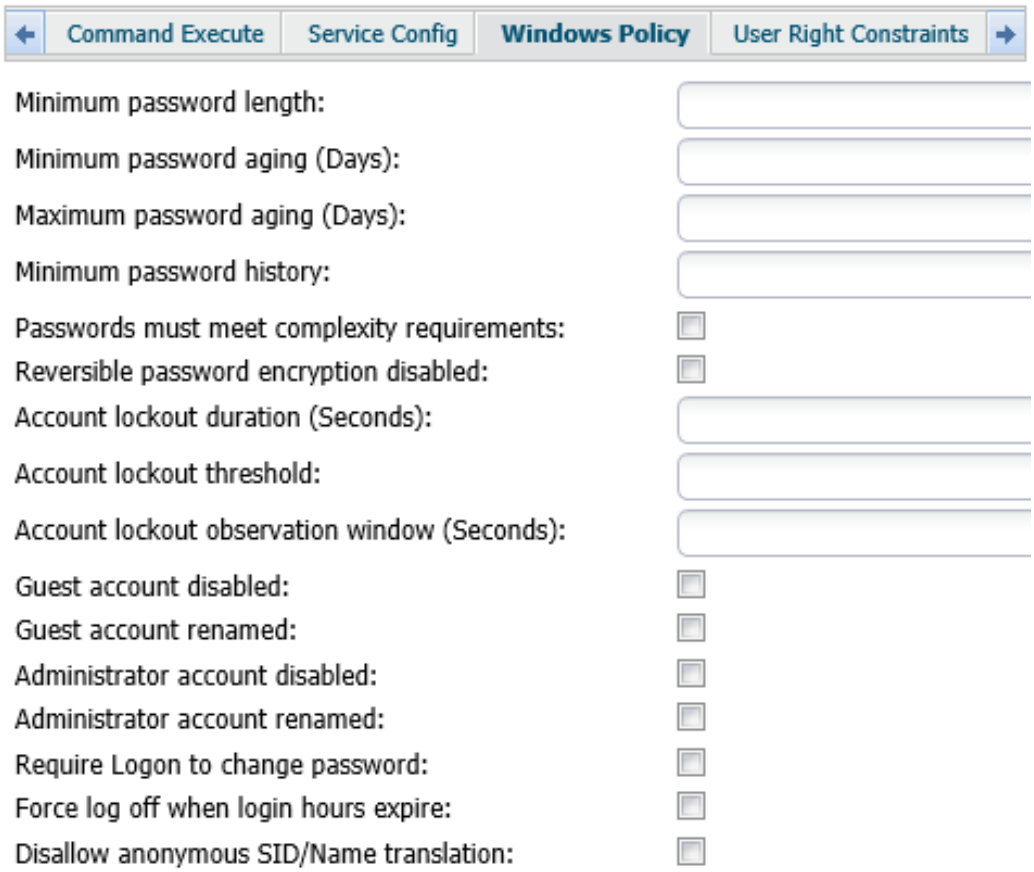
The **Service Config** tab checks the levels of the services running on a Red Hat systems.



Option	Description
Name	Name of the service.
Levels	Define the level or levels of the service.
Status	If the service should be enabled or disabled.
Description	Description of the check.

Windows Policy Tab

The **Windows Policy** tab is a rule set for passwords and default accounts on Windows systems, and describes password length, aging, password history, and so forth.

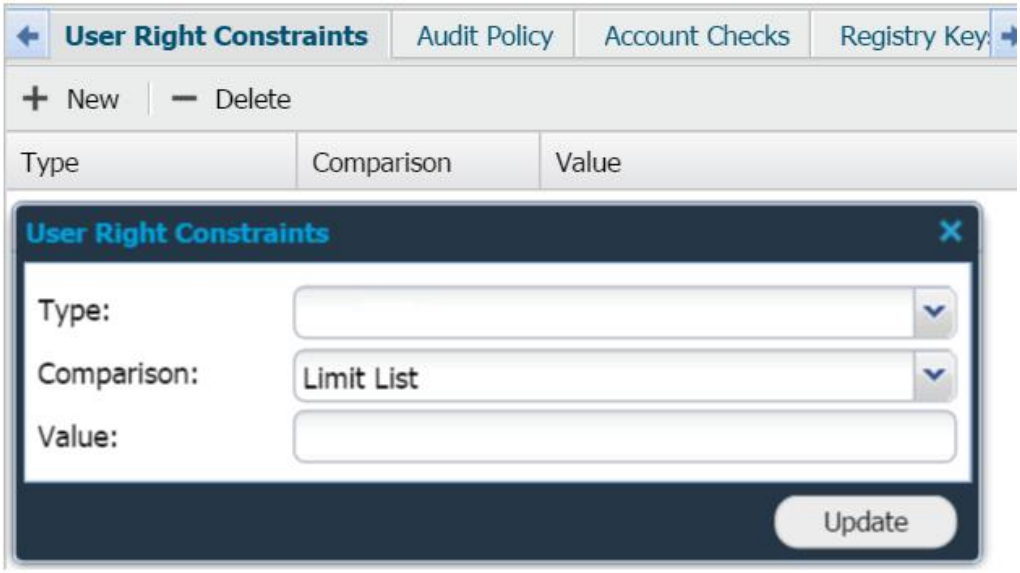


Option	Description
Minimum password length	The minimal length of the password.
Minimum password aging (Days)	Minimum number of days after the password can be changed.
Maximum password aging (Days)	Maximum number of days after the password must be changed.
Minimum password history	Number of previous passwords that the user can't use.
Passwords must meet complexity requirements	Tests, when enabled, if passwords meet the password complexity requirements.

Option	Description
Reversible password encryption disabled	Tests, when enabled, if reversible password encryption is disabled.
Account lockout duration (Seconds)	The amount of time, in seconds, that an account can be locked due to Lockout-Threshold being exceeded.
Account lockout threshold	Maximum number of invalid logon attempts that are permitted before the account is locked out.
Account lockout observation window (Seconds)	The range of time, in seconds, in which the system increments the number of incorrect logon attempts.
Guest account disabled	Enabling this will add checks to test if account for ‘Guest’ user is disabled.
Guest account renamed	Enabling this will add checks to test if account for ‘Guest’ user is renamed.
Administrator account disabled	Enabling this will add checks to test if account for ‘Administrator’ user is disabled.
Administrator account renamed	Enabling this will add checks to test if account for ‘Administrator’ user is renamed.
Require Logon to change password	Enabling this will add checks to test if it is required to be logged in to change the password.
Force log off when login hours expire	Enabling this will add checks to test if the user is logged off when the login hours has expired.
Disallow anonymous SID/Name translation	Enabling this will add checks to test if anonymous SID/Name translation is disallowed.

User Right Constraints Tab

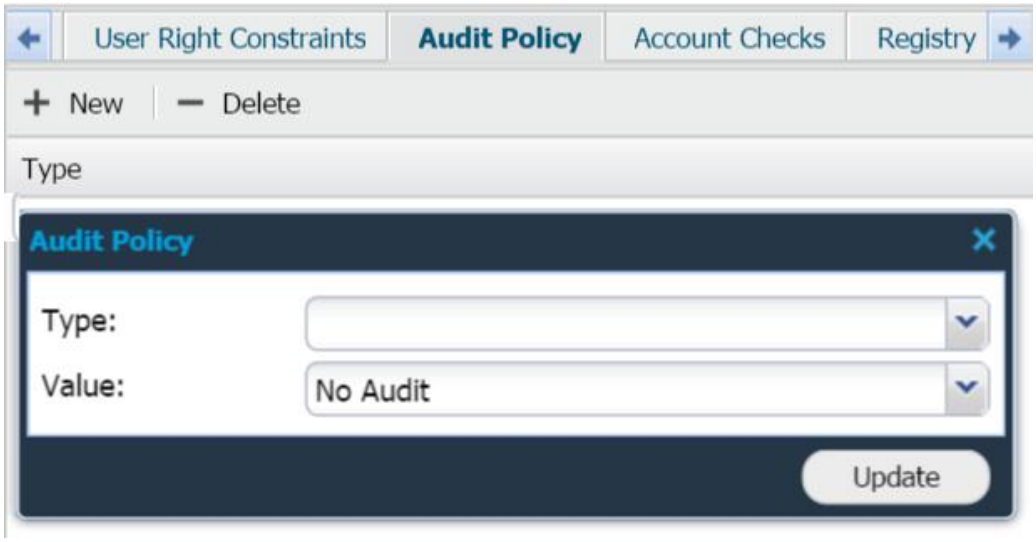
The **User Right Constraints** tab define what value a user right should have.
***Note**: Only applicable in Windows.*



Option	Description
Type	Define the right.
Comparison	Choose between: ► Equals ► In List ► Limit List
Value	If the right should be *Enabled* or *Disabled*.

Audit Policy Tab

The **Audit Policy** tab defines the audit policy and when the audit event is generated.
***Note**: Only applicable in Windows.*



Option	Description
Type	Define the Audit Policy. ► System ◆ Security System Extension ◆ System Integrity ◆ IPsec Driver ◆ Other System Events ◆ Security State Change ► Logon/Logoff ◆ Logon ◆ Logoff ◆ Account Lockout ◆ IPsec Main Mode ◆ IPsec Quick Mode ◆ IPsec Extended Mode ◆ Special Logon ◆ Other Logon/Logoff Events ◆ Network Policy Server ◆ User / Device Claims ► Object Access ◆ File System ◆ Registry ◆ Kernel Object ◆ SAM ◆ Certification Service

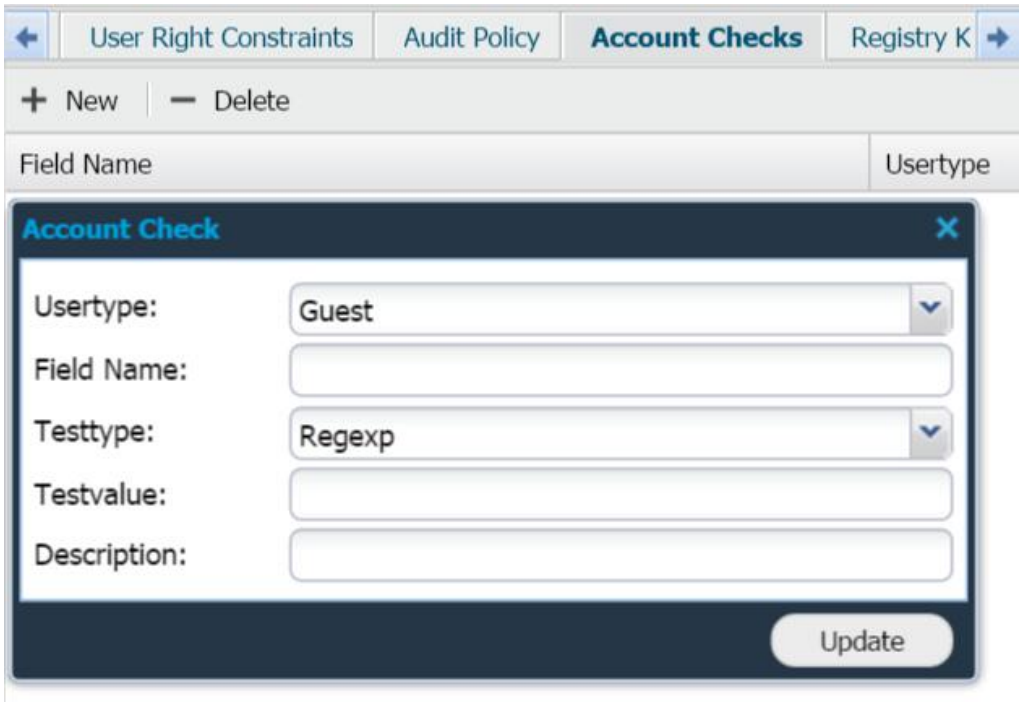
Option	Description
	◆ Application Generated ◆ Handle Manipulation ◆ File Share ◆ Filtering Platform Packet Drop ◆ Filtering Platform Connection ◆ Other Object Access Events ◆ Detailed File Share ◆ Removeable Storage ◆ Central Policy Staging ► Privilege Use ◆ Sensitive Privilege Use ◆ Non Sensitive Privilege Use ◆ Other Privilege Use Events ► Detailed Tracking ◆ Process Termination ◆ DPAPI Activity ◆ RPC Events ◆ Process Creation ► Policy Change ◆ Audit Policy Change ◆ Authentication Policy Change ◆ Authorization Policy Change ◆ MPSSVC Rule-Level Policy Change ◆ Filtering Platform Policy Change ◆ Other Policy Change Events ► Account Management ◆ User Account Management ◆ Computer Account Management ◆ Security Account Management ◆ Distribution Group Management ◆ Application Group Management ◆ Other Account Management Events ► DS Access ◆ Directory Service Changes ◆ Directory Service Replication ◆ Detailed Directory Service Replication ◆ Directory Service Access ► Account Logon ◆ Kerberos Service Ticket Operations ◆ Other Account Logon Events ◆ Kerberos Authentication Service ◆ Credential Validation

Option	Description
Value	Choose between: ► No Audit ► Success ► Success Allow Failure ► Failure ► Failure Allow Success ► Success, Failure

Account Checks Tab

The **Account Check** tab checks if account exists.

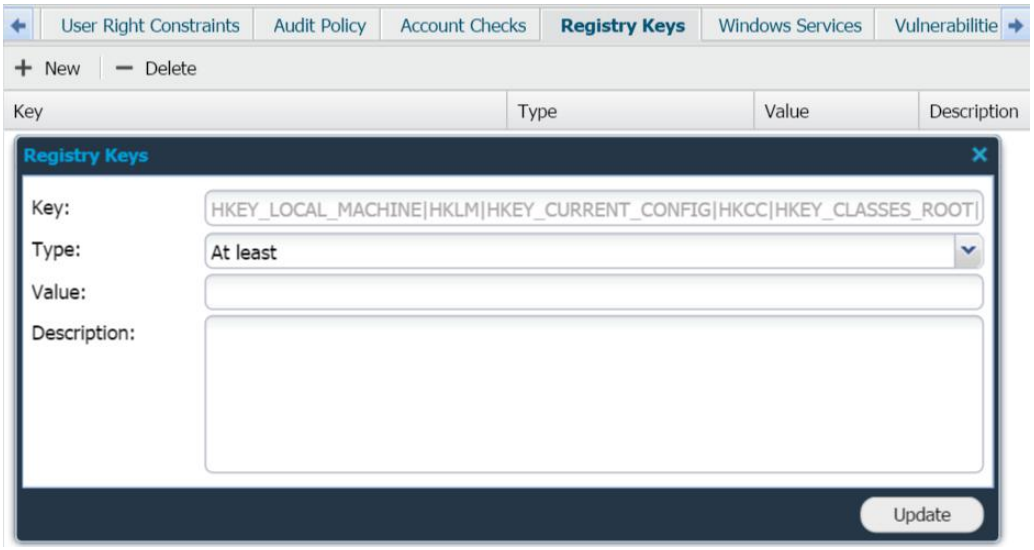
***Note**: Only applicable in Windows.*



Option	Description
Usertype	Choose between: ► Any ► Guest ► User ► Admin
Field Name	Define which structure you wish to check against for the usertype.
Testtype	Choose between: ► Regexp ► Bit And
Testvalue	The value of the structure.
Description	Description of the check.

Registry Keys Tab

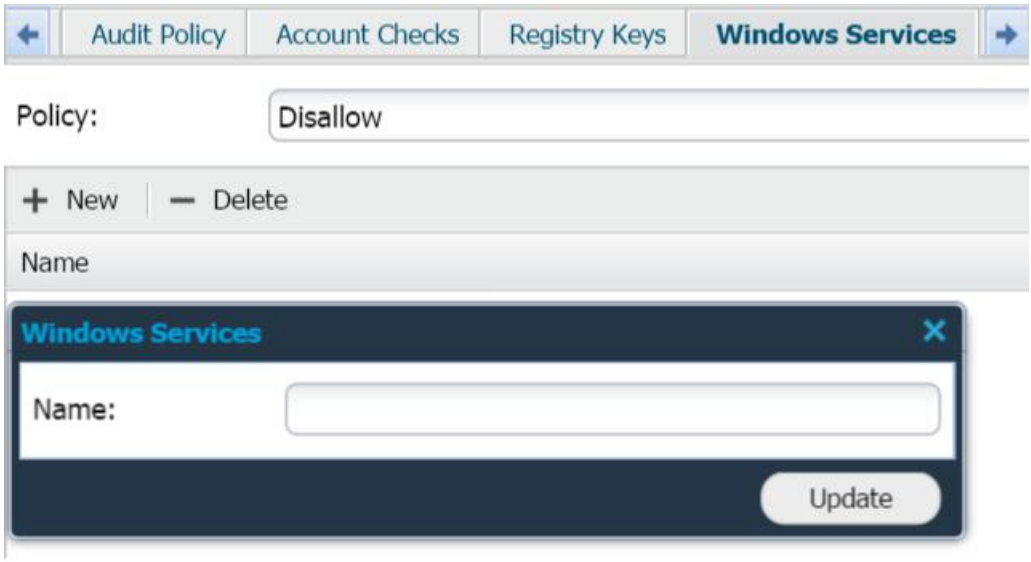
Define policy on Windows keys and their values.



Option	Description
Key	Define the Windows key.
Type	Choose between: ► Reqexp ► Equals ► Equals allow missing ► At least ► At least allow missing ► At most ► At most allow missing ► Not set ► Not empty
Value	The value for the Windows key.
Description	Description of the check.

Windows Services Tab

The **Windows Services** tab *allow, disallow* and *exactly* Windows services or define exactly what services that the system should contain.

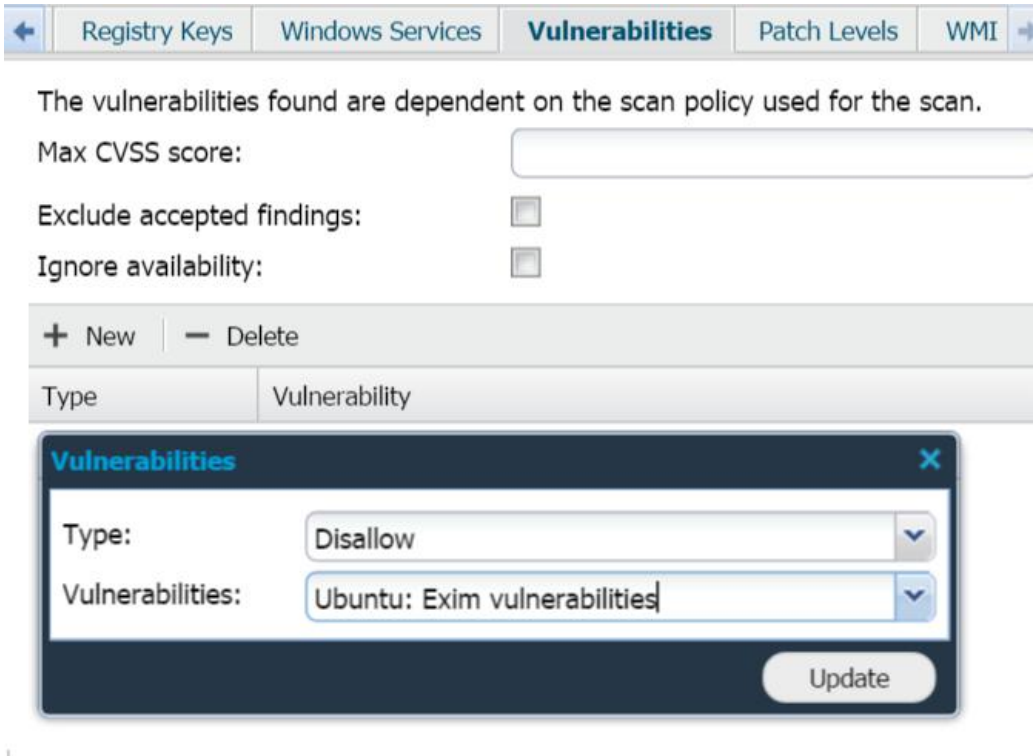


Option	Description
Policy	Choose between: ► Disallow ► Allow ► Exactly
Name	Name of the service.

Vulnerabilities Tab

The **Vulnerabilities** tab define the maximum CVSS score which the targets can have. The vulnerabilities found are dependent on the scan policy used for the scan.

***Note**: When running a Compliance Only scan, this will not be triggered.*

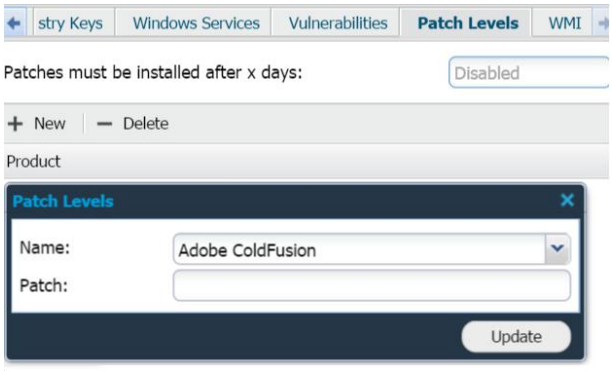


Option	Description
Max CVSS score	Define the maximum CVSS scoring allowed on the target.
Exclude accepted findings	Enable to exclude all accepted findings.
Ignore availability	Enable to ignore a vulnerability which only has an availability impact.
Type	Choose between: ► Disallow ► Require
Vulnerabilities	Define the vulnerability that should be required or disallowed on the target.

Patch Levels Tab

The **Patch Levels** tab defines which patch level the application should have.

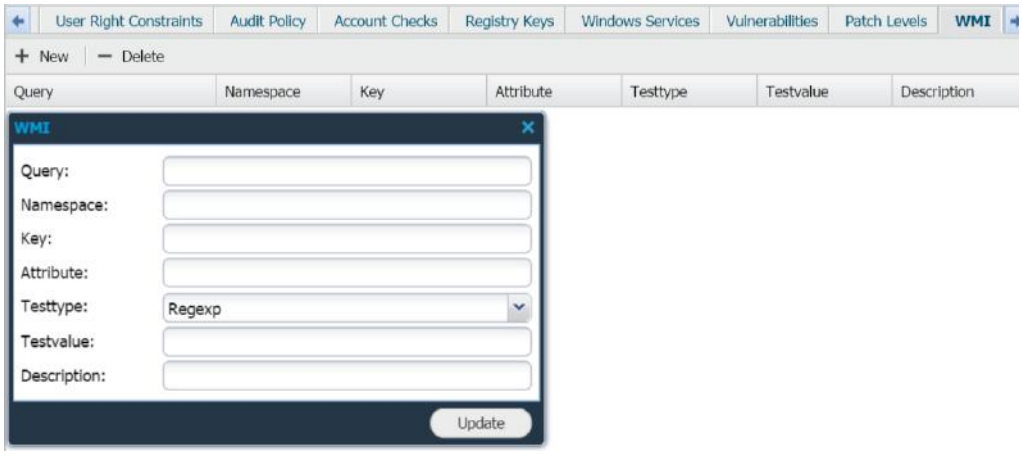
***Note**: When running a Compliance Only scan, this will not be triggered.*



Option	Description
Patches must be installed after x days	Define the number of days.
Name	Define which application.
Patch	Define the patch level.

WMI Tab

The WMI tab defines WMI queries to be executed on the target. This check will fail if the query matches the **Testvalue**.

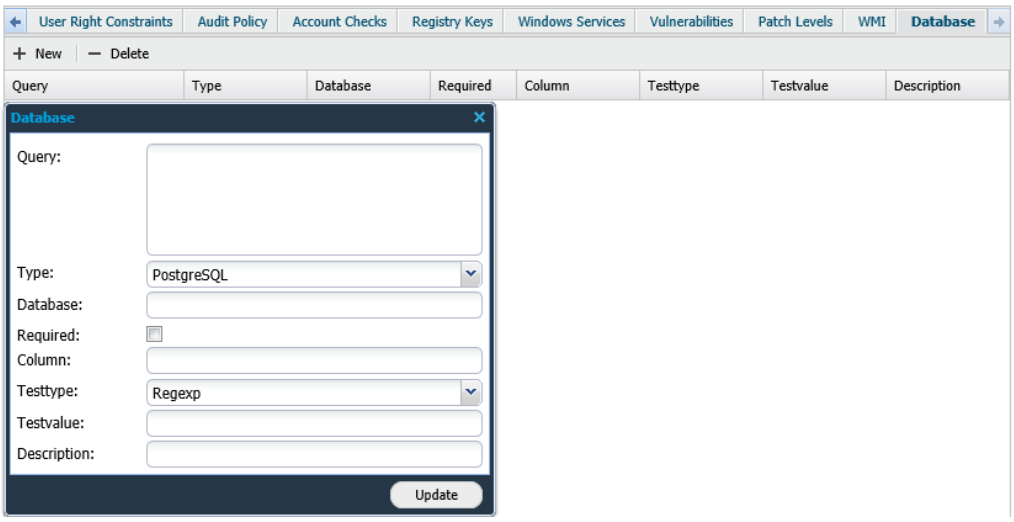


Option	Description
Query	'SELECT' query in WMI query language.
Namespace	WMI namespace name.
Key	The key to present the given attribute in report.
Attribute	Name of the column that should be tested in the result of the given query.
Testtype	Choose between: ► Regexp ► Bit And ► Inverse Regexp
Testvalue	The value to compare against the results of the query.
Description	Description of the check.

Database Tab

The **Database** tab defines database queries to be executed on the target. This check fails if the query matches the test value.

***Note**: This check requires that database authentication is configured on the target. This is described in detail in chapter 0 Database Authentication*



Option	Description
Query	'SELECT' database query
Type	Choose between: ► PostgreSQL ► MySQL ► DB2 ► Oracle ► MS SQL
Database	Define which database this query should be executed in.
Required	Will run the test even if no database exists on the target.
Column	Name of the column that should be tested in the result of the given query.
Testtype	Choose between: ► Regexp ► Equals ► Not equals
Testvalue	The value that should be checked for.
Description	Description of the check.

Inherit Policy

Inheriting a policy is done by using the *Inherit Policy* option. This toggle a new window with a drop-down menu in which a predefined policy can be chosen from which to inherit from. This option is also available by right clicking any entry within the Requirements Tree, and choosing *Inherit Policy*.

Policies provide prescriptive guidance for establishing a secure configuration posture for the system the policy is constructed for. By inheriting a policy, a number of known requirements are predefined and makes the setup of a scan easier, also making sure that known vulnerabilities are not overlooked.

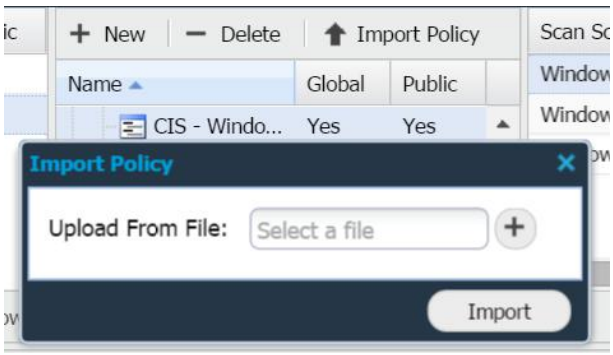
By inheriting a compliance policy, you get all the defined requirements/questions in to the policy you are inheriting to. You can always add more requirements/questions to the new policy.

Remove Policy

Removing a policy is done by selecting the policy to remove, and click **Delete** in the upper left corner of the *Compliance Module*, or by right clicking the policy directly and choosing **Delete**. To only remove a specific requirement for a policy, right click the policy, choose **Edit**, right click the requirement you wish to remove, and choose **Delete**. It is not possible to remove any pre-defined compliance policy, only the policies listed within the *Custom* directory.

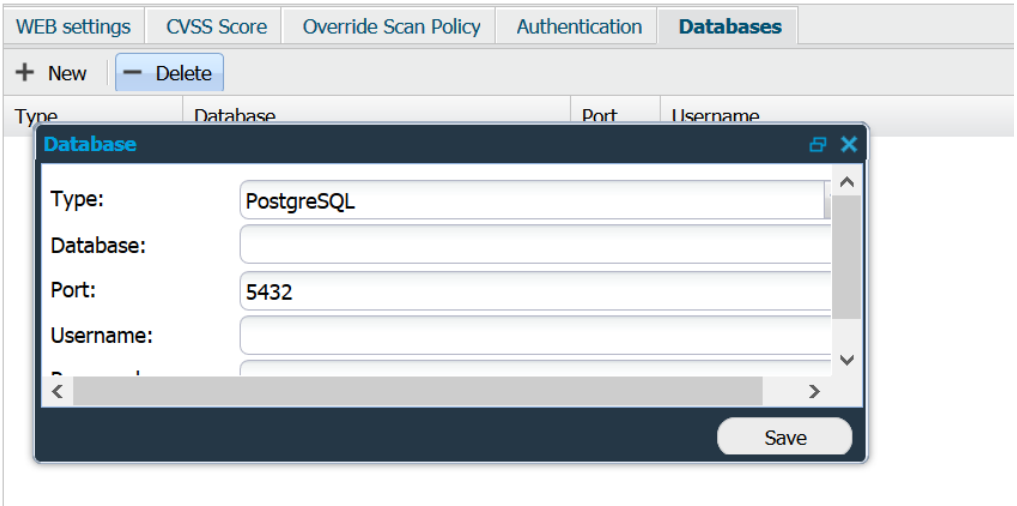
Import and Export Policy

Exporting a policy is done by right clicking the policy to export, and choose **Export Policy**. This export the policy in .xml format.
Importing a policy is done by using **Import Policy** within the *Policy* section, choose which policy to import and press **Import**.



Database Authentication

Database authentication is defined on the target within *Manage Targets*.
Right click the target you wish to authenticate against, choose *Edit* and go to the **Databases** tab.



To add credentials to be used click **New** and defined the following:

Option	Description
Type	Type of the database, choose between *PostgreSQL*, *MySQL*, *DB2,* and *Oracle.*
Database	Define which database the scanner should connect to.
Port	Define which port the scanner should connect on.
Username	Define the username used for the authentication.
Password	Define the password used for the authentication.

2.2.3 Scan Schedule Grid

The Scan Schedule grid lists the scans that has been executed with the compliance box checked, displays what date the scan schedule was executed, and determines which scan schedule results that should be presented in the lower section.

2.2.4 Target Group Grid

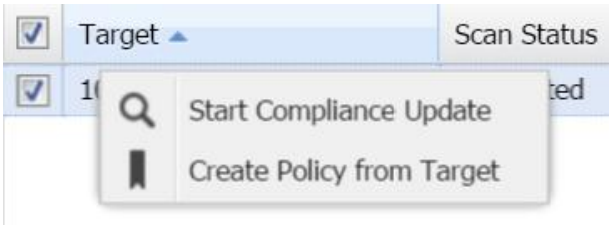
The Target Group grid lists the target groups which has been defined within the system, from which you can choose the target group that you wish to present results for in the lower section.

2.2.5 Target Grid

The Target grid displays all targets in the selected Target Group. Choose the targets within the target group that you wish to display in the lower section.
This grid will also show if the targets listed are compliant or not within the *Compliant* column, based on the policy chosen within the Compliance Policy grid:

- - Compliant
- - Not compliant

Right clicking any target allows you to choose one of these two options:



Option	Description
Start Compliance Update	Recheck registry keys on the selected target, instead of running a full scan.
Create Policy from Target	Create a compliance policy based on the selected target.

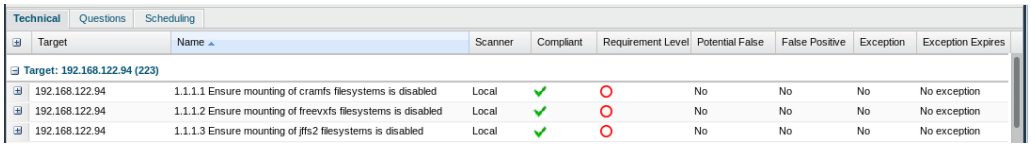
2.3 Interface Lower Section

The lower section presents the compliance report based on the options selected in the top section, and consists of three tabs.

- Technical tab
- Questions tab
- Scheduling tab

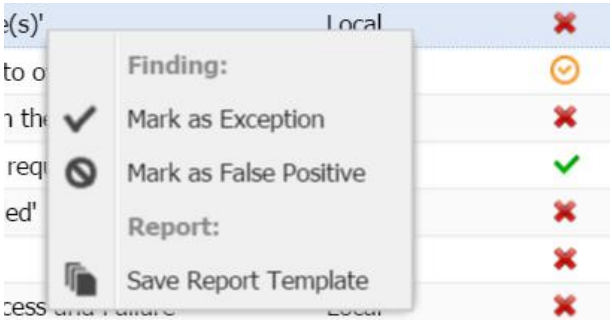
2.3.1 Technical Tab

The **Technical** tab presents all the results from the scanning, and is fully configurable. To customize what columns to show, click the arrow next to the column name and choose from the options presented in the table.



Option	Description
Compliant	Shows if the result is compliant or not. - Not Compliant - Compliant - Marked as an exception
Exception	*Yes,* if the result has been marked as an exception.
Exception Expires	Date when the exception expires.
False Positive	*Yes,* if the result has been marked as a False Positive.
Host Name	The targets host name.
Name	The name of the requirement/control.
Platform	The targets platform.
Potential False	Displays if the result is a potential false positive.
Requirement level	Shows the level of the requirement. - None - Best Practice - Critical
Scanner	Which scanner the scan was executed on. Only visible if at least one scanner is registered.
Target	The targets IP address.

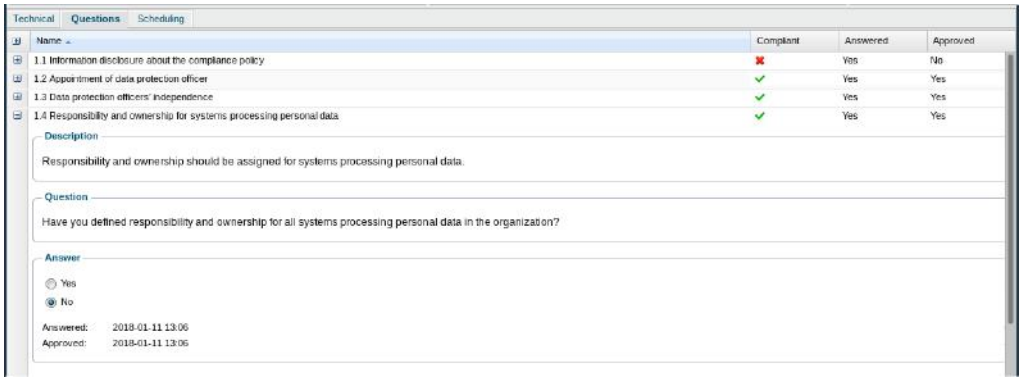
Right clicking any result allow you to choose one of the following three options:



Option	Description
Mark as Exception	Mark a result which is not compliant as an exception. Only available for non-compliant results.
Mark as False Positive	Mark a result as a False Positive. Checking *Send Information to the Outpost24 Vulnerability Research and Development Team* forward this False Positive for investigation to the Outpost24 Team. Only available for non-compliant result.
Save Report Template	Saves the current filtering as a Report Template.

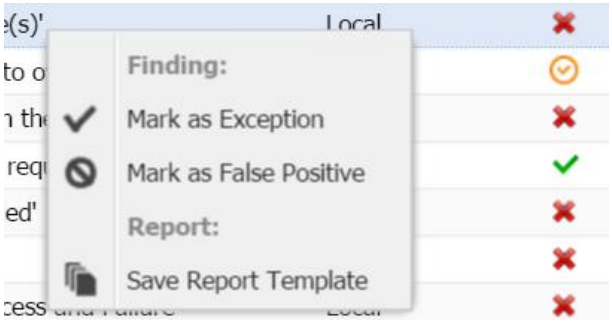
2.3.2 Question Tab

The **Question** tab, presents all the compliancy questions that need to be answered and approved to be compliant. To customize what columns to show, click the arrow next to the column name and choose from the options presented in the table.



Option	Description
Answered	Shows if the question has been answered
Approved	Shows if the answered question has been approved
Compliant	Shows if the finding is compliant or not. - Not Compliant - Compliant - Marked as an exception
Name	The name of the requirement/control.

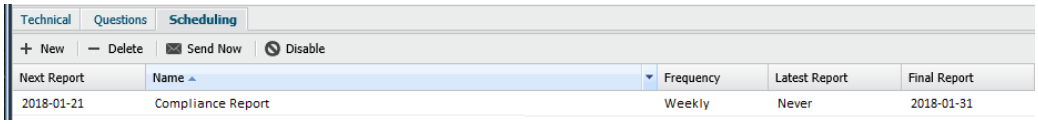
Right clicking any finding allows you to choose one of the following three options:



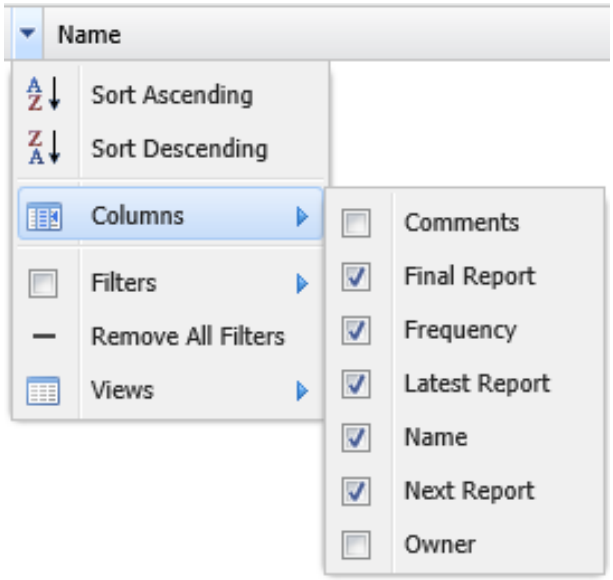
Option	Description
Mark as Exception	Mark a finding which is not compliant as an exception. Only available for non-compliant findings.
Mark as False Positive	Mark a finding as a False Positive. Checking *Send Information to the Outpost24 Vulnerability Research and Development Team* forward this False Positive for investigation to the Outpost24 Team. Only available for non-compliant findings.
Save Report Template	Saves the current filtering as a Report Template.

2.3.3 Scheduling Tab

The **Scheduling** Tab allows for maintenance of already existing scheduled reports or creation of new scheduled reports to be sent out on the defined schedule timing.



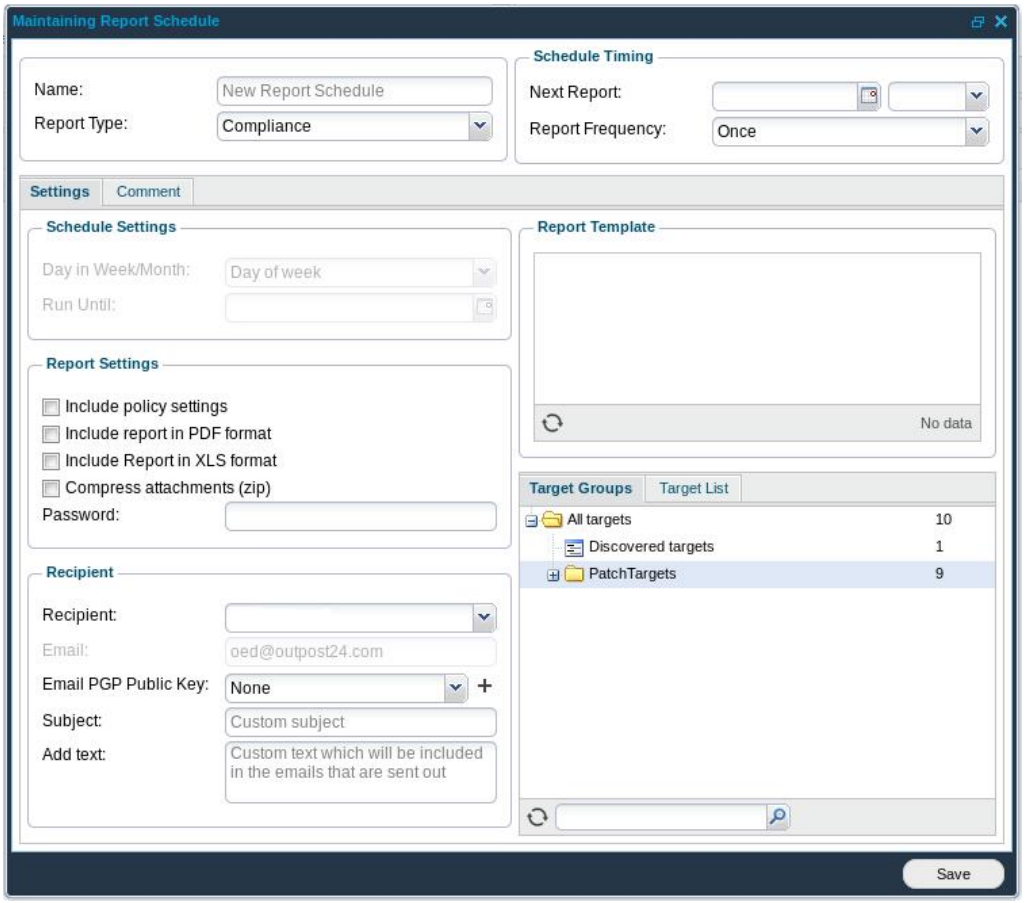
The Scheduled Reports grid is configurable. Clicking the arrow next to the name of any grid column allows for customization of which of the following columns that will be displayed:



Option	Description
Comments	Comments about the report.
Final Report	On what date, the final report is sent.
Frequency	How frequently the report should be generated.
Latest Report	Last time the report was generated.
Name	Name of the report.
Next Report	The next time when the report will be generated.
Owner	The owner of the report.

Create New Scheduled Report

New in the upper left corner toggle a new window, *Maintaining Report Schedule*, which presents various options on how to schedule the compliance reports.



Schedule Timing

Settings to configure how frequently the report should be sent:

Option	Description
Next report	Define the next time when the report should be scheduled. For example, next Monday.
Report Frequency	Define how frequently the report should be sent out. For example, every Monday. **Once** – Only send the report once **Weekly** – Every week, starting on the day set in *Next Report*. **Monthly** – Every month, starting on the day set in *Next Report.* **Bimonthly** – Every second month, starting on the day set in *Next Report.* **Quarterly** – Every third month, starting on the day set in *Next Report*. **Fortnightly** – Every second week, starting on the day set in *Next Report*. **Daily** – Every day, starting on the day set in *Next Report.*

Schedule Settings

The *Schedule Settings* are activated depending on the value of the *Report Frequency*. It allows you to configure what day in week or month the report should run.

- Day of week
- Day of month
- Day of week in month

Run Until allows you to set an end date for when the report period should end.

Report Settings

This section gives you the option to choose if you wish to include the policy settings in the compliance report, if the report should be in PDF, XLS format or both, compress attachment in a zip format, and if the file should be password protected or not.

Recipient

Choose between sending the report to any of the defined users within the system, or *Custom* for which main account users or super user can define the email address to send the report. It is also possible to choose between *encrypting* the email with a public PGP key, or *no encryption*.
This section also gives you the option to customize the email that are sent out with the compliance reports. If nothing is entered the pre-defined text will be used.

Report Template

Choose the report template that you wish to use. Report Templates are created within the Compliance Module by filtering findings on columns, right clicking any entry within the findings grid and choosing *Save Report Template*.

Target Groups

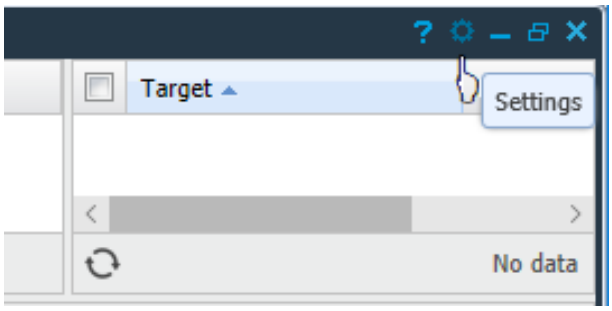
Choose which Target Group the report should include.

Target List

Choose which targets, from the target group, the report should include.

2.4 Privacy Settings

To access the settings window, click the cogwheel in the upper right corner.



In **Settings**, the *Compliance Policy Ownership* can be set to either **Public** or **Private**. This setting determines if the policies will be visible for all users within the tool by default, or only for the user who created the policy.