

Management Portal Extended / Industrial Vulnerability Manager

System Manual

<u>Introduction</u>	1
<u>Overview of the Tabs of the User Interface</u>	2
<u>Using the Industrial Vulnerability Manager</u>	3
<u>Settings</u>	4
<u>Change History</u>	A

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction	5
1.1	Health Note	5
1.2	Security information	5
1.3	Screenshots and Graphics	6
1.4	New Naming.....	6
1.5	Introduction	6
2	Overview of the Tabs of the User Interface.....	9
2.1	Tabs Overview	9
2.2	Dashboard User Interface.....	12
2.3	Inventory User Interface.....	13
2.4	Vulnerabilities User Interface.....	14
2.5	Detail View of Vulnerabilities.....	15
2.6	Tasklist User Interface	19
2.7	Settings User Interface.....	20
3	Using the Industrial Vulnerability Manager	21
3.1	Checking Components for Vulnerabilities	21
3.1.1	Creating a New Device or Product and Adding Components Individually	21
3.1.1.1	Creating New Device or Product	21
3.1.1.2	Adding Individual Components	22
3.1.2	Importing a list with multiple components	24
3.1.2.1	Importing a File	25
3.1.2.2	Creating a CSV File.....	26
3.2	Assigning a Status to Vulnerabilities	28
3.3	Exporting Monitoring Lists	30
3.4	Using the Tasklist.....	31
3.5	Using Dashboard Filter Options	32
4	Settings.....	33
4.1	Profile.....	33
4.1.1	Account.....	33
4.1.2	Subscription	33
A	Change History	35

Introduction

1.1 Health Note

Epilepsy note

Some people may experience epileptic seizures when exposed to certain light frequencies, flickering light sources or geometric shapes and patterns. Certain light frequencies in screen backgrounds or in certain applications can trigger an epileptic seizure in these people.

1.2 Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

Changes based on our recommendations needs to be validated on an adequate Test System at first.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

1.3 Screenshots and Graphics

The screenshots and graphics used in this document serve as examples only. They do not reflect all the possible inputs and sources. Rather, they are informative in nature and are provided to improve understanding. Parameters for the configuration can be taken from the texts and tables and depend on the individual system.

1.4 New Naming

Since end of 2022 Industrial Vulnerability Manager is part of the Vilocify Vulnerability Services. In August 2023 the naming of all 3 products within VVS were changed. IVM is now named as Management Portal Extended. This change effects mainly the order management. The naming Industrial Vulnerability Manager is still being used in the actual version. Find out more about the Vilocify Vulnerability Services here: <https://www.siemens.com/vvs>

1.5 Introduction



Industrial Vulnerability Manager is an application that is offered on different cloud platforms as well as on Siemens Edge.

Note

We recommend using the Google Chrome web browser to ensure fault-free use of Industrial Vulnerability Manager.

You can use the Industrial Vulnerability Manager to create software component lists for your products or existing devices.

You add software and firmware versions (components) to your lists and monitor them in order to obtain an overview of known vulnerabilities at all times.

Once you have created your components, they are compared with daily updated vulnerability information. All known vulnerabilities that can affect your components are displayed.

The vulnerabilities are listed in a table. In addition to assigning a status, the table also provides detailed information about the vulnerability. A date can be selected and comments can be left for the processing of the vulnerabilities.

The "Tasklist" displays vulnerabilities with assigned date in chronological order and divides them into two groups: "Overdue Fixes" and "Upcoming Fixes".

You can use the "Subscription" function to receive regular updates on newly detected vulnerabilities.

The "Dashboard" provides an overview of all components and their vulnerabilities in the form of diagrams.

Overview of the Tabs of the User Interface

2.1 Tabs Overview

This section provides you with an overview of the tabs of the user interface of Industrial Vulnerability Manager.

- "Dashboard"
- "Inventory"
- "Vulnerabilities"
- "Tasklist"
- "Settings"

Dashboard tab

The "Dashboard" is the home page of Industrial Vulnerability Manager and provides an overview of all components and their vulnerabilities in the form of diagrams.

The "Dashboard" features the following diagrams:

- A status diagram that shows how many open, closed, analyzed and acknowledged vulnerabilities are present.
- A priorities diagram that shows components by priority (critical, major, minor, etc.) and their number.
- A patch status diagram that displays the vulnerabilities according to patch status (not defined, official fix, temporary fix, etc.).
- A time diagram that shows the distribution of the different status of vulnerabilities over a period of time.

Inventory tab

The "Inventory" tab provides you with the following options:

- Create and sort lists individually
- Create, sort and edit lists for devices or products or store information
- Add one or more components to a list
- Import a list of multiple lists and components via a file in the appropriate format (.csv, .xlsx, .json or .aml).

2.1 Tabs Overview

- Export lists with 2 choices:
 - "Export monitored"
 - "Export unmonitored"
- Download the report "Vulnerability Manager Report" with the following content for selected lists:
 - Device overview
 - Vulnerability overview of the individual components broken down by device or product

Vulnerabilities tab

All vulnerabilities are listed in the "Vulnerabilities" tab. Each vulnerability can be assigned a status.

Four status options are available for the assignment:

- Open
- Analysis Ongoing
- Closed
- Acknowledged

The status "Open" is automatically assigned to each new vulnerability. This vulnerability has not yet been viewed or addressed.

The status "Analysis Ongoing" contains the vulnerabilities that are currently being processed or monitored.

The status "Close" contains the vulnerabilities that have been remedied and are considered to have been successfully resolved.

The status "Acknowledged" contains the vulnerabilities that have been acknowledged but deliberately left unresolved and therefore carry a risk.

The displayed vulnerabilities can be filtered and exported as an Excel file.

Under "Details" you will find a detailed description of each component and vulnerability. The detailed description can be commented and printed. In the detail view, you can also define the status and the processing time for the vulnerability. The processing of the vulnerability can also be assigned to a person.

Tasklist tab

In the "Tasklist" tab you will find a chronological overview of the vulnerabilities to be processed. You can also see the vulnerabilities that have been assigned to specific persons and you can sort the vulnerabilities by name of the person.

From here you can go to the detail view of the respective vulnerability. In the detail view, you can obtain detailed information on the vulnerability, redefine the status of the vulnerability, select a different processing date, assign the processing of the vulnerability to a person, or leave a new comment.

Settings tab

You have the following options in the "Settings" tab:

- "Profile" > "Account" menu:

Here you can change your password yourself.

- "Profile" > "Subscription" menu:

Here you can activate the email notification, so that you are informed regularly about new vulnerabilities.

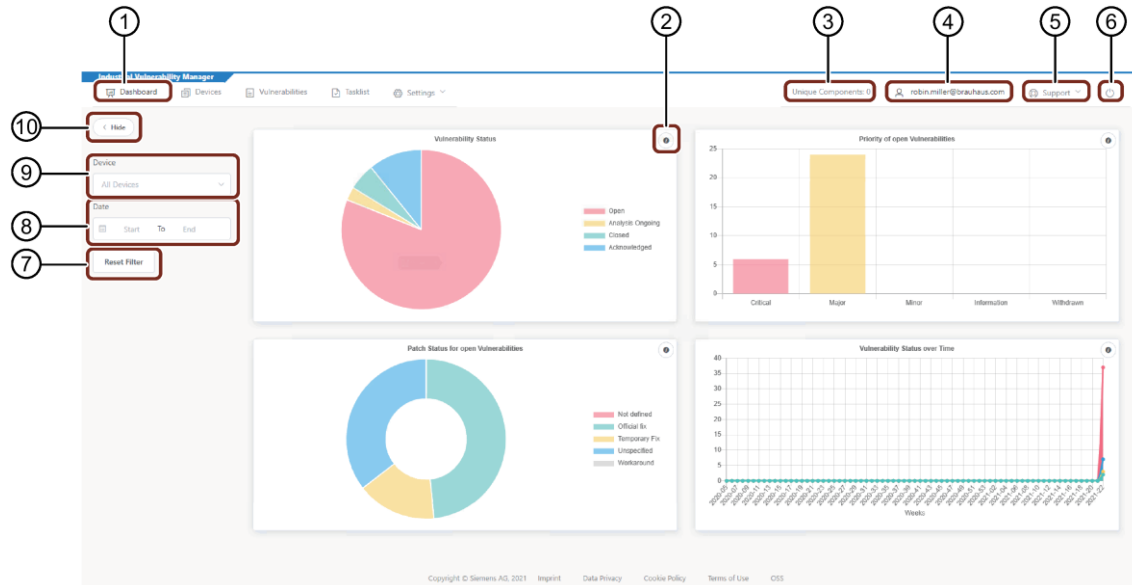
See also

Using the Industrial Vulnerability Manager (Page 21)

2.2 Dashboard User Interface

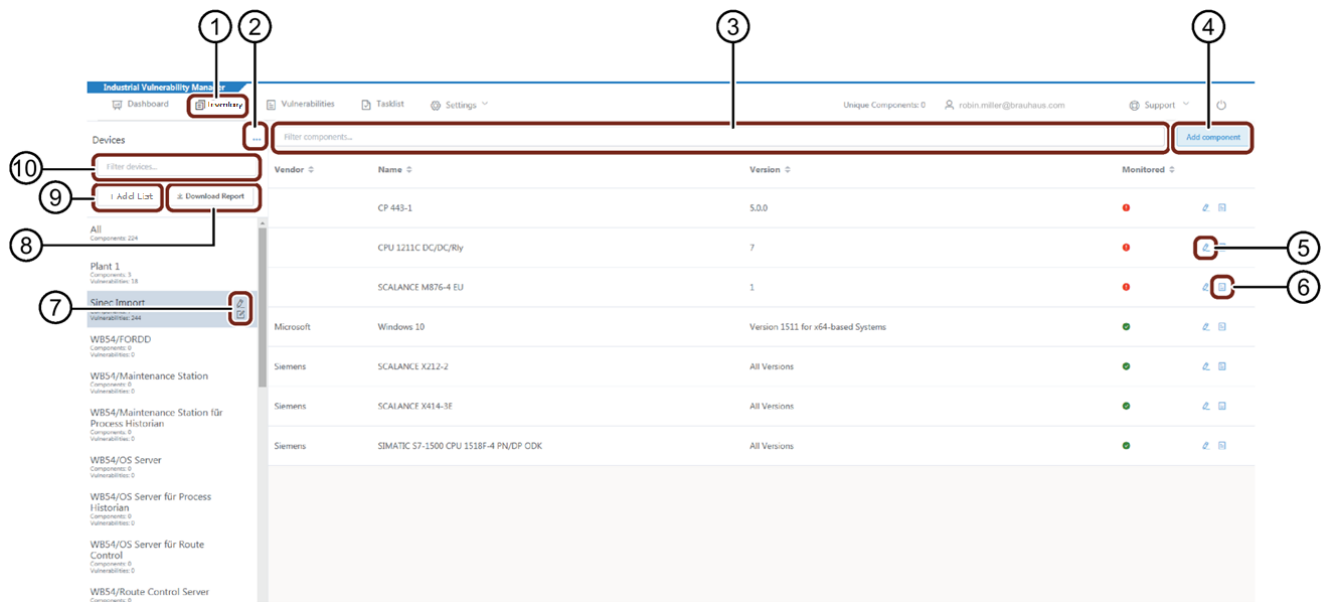
Once you have logged on to the Industrial Vulnerability Manager, the "Dashboard" tab with its user interface is the homepage of the application at the same time.

The top menu line is identical for all tabs and is therefore described once in this section.



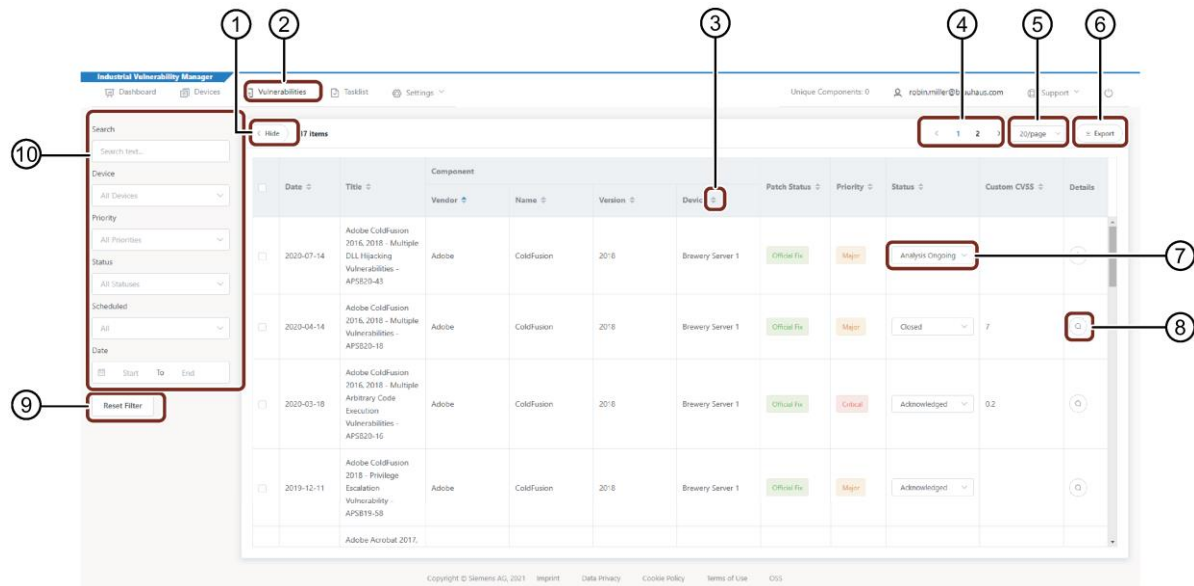
- ① Active tab "Dashboard"
- ② Open info field with mouseover function
- ③ Number of unique components for licencing
- ④ Jump to menu "Settings" > "Account"
- ⑤ Open the drop-down menu: "Mail" and "User Documentation"
- ⑥ Log out
- ⑦ Reset filter
- ⑧ Select period
- ⑨ Select device or product
- ⑩ Show and hide filter options

2.3 Inventory User Interface



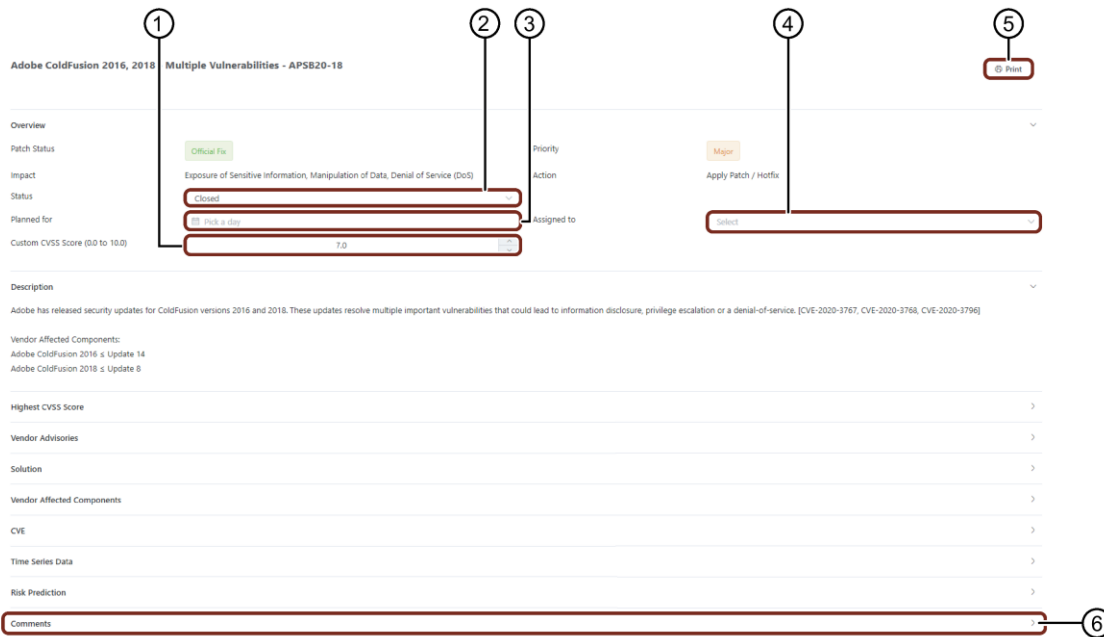
- ① Active tab "Inventory"
- ② Open the drop-down menu:
 - Import and export from lists (components)
 - Select view: List and Hierarchy view
- ③ Filter components by name
- ④ Add individual components
- ⑤ Edit or delete components
- ⑥ Go to vulnerabilities of the component
- ⑦ Open icon with mouseover function:
 - Edit device list
 - Leave information about the device list
- ⑧ Generate and download report for selected list
- ⑨ Add a new list
- ⑩ Filter lists by name

2.4 Vulnerabilities User Interface



- ① Hide filter options
- ② Active tab "Vulnerabilities"
- ③ Determine sorting
- ④ Page selection
- ⑤ Number of vulnerabilities per page
- ⑥ Export displayed vulnerabilities to page
- ⑦ Select status of the vulnerability
- ⑧ Open detail view of the vulnerability
- ⑨ Reset filter
- ⑩ Filter options

2.5 Detail View of Vulnerabilities



- ① Assign a custom CVSS score from 0 to 10
- ② Assign status
- ③ Select processing date
- ④ Assign vulnerability to a person for processing
- ⑤ Print details
- ⑥ Leave a comment

Description

Description of the specified vulnerability. Provides technical information and, if available, a specification of the vulnerability.

Highest CVSS Score

Shows the highest CVSS score.

Vendor Advisories

Provides a link to vendor advisories regarding the specified vulnerability.

Solution

Provides information about official solutions and workarounds.

Vendor Affected Components

List of all vendor affected components.

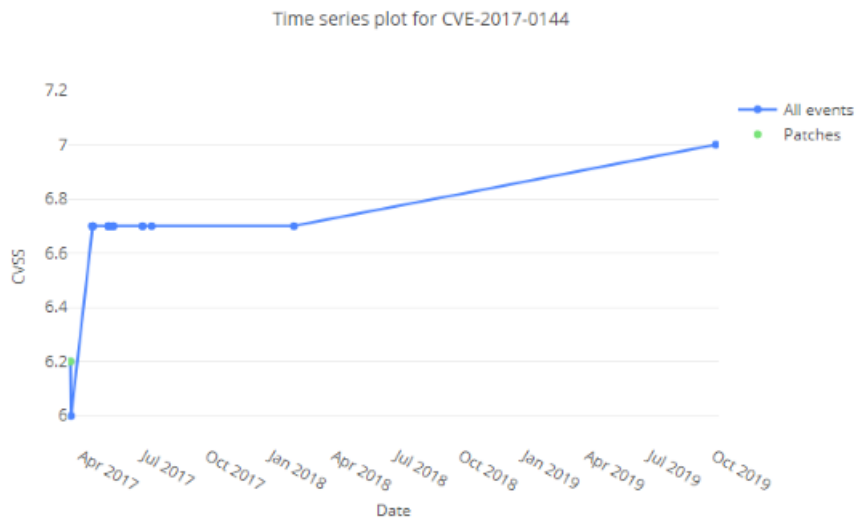
CVE (Common Vulnerabilities and Exposures)

Provides a link to the National Vulnerability Database. The database provides additional information, like known affected software configurations

Comments

You can leave comments on a specified vulnerability.

Time Series Data



The Time Series Graph shows the development of the CVSS Score affected by the events over a period of time.

Each event consists of the following fields:

- Exploitability Level

The "Exploitability Level" describes the level of an existing exploit as follows:

- "Unproven": Known theoretical exploitability, not yet proven.
- "Proof of Concept": Proof of concept exists.
- "High": High level of exploitability. Exploit actively used in the wild.

- Patch Status

The "Patch Status" describes the level of available patches as follows:

- "Unavailable": A patch is not yet available.
- "Temporary Fix": A temporary fix is available.
- "Official Fix": An official fix is available.

- Vulnerability Status

The "Vulnerability Status" describes the status of the vulnerability as follows:

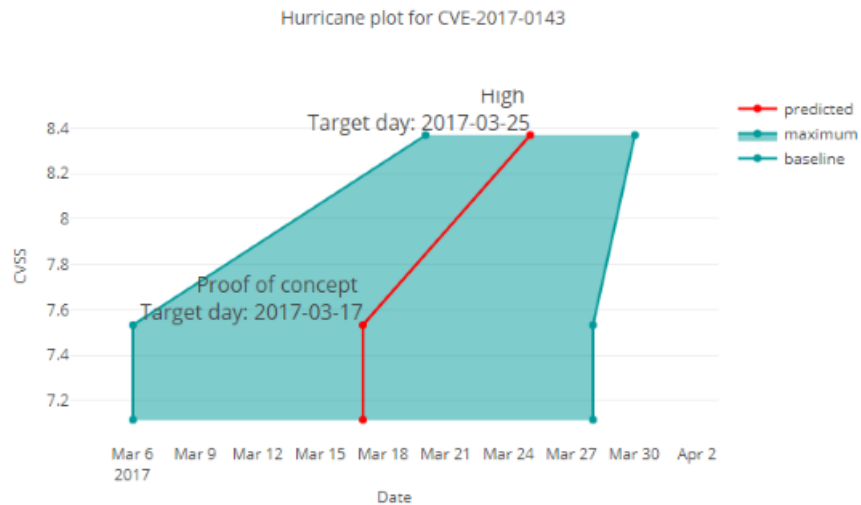
- "Reasonable": The vulnerability is on a theoretical level and has not yet been confirmed.
- "Confirmed": the vulnerability has been confirmed.

- Source

"Source" describes the source of the event as follows:

- NIST Disclose
- Vendor
- Third Party
- Weaponization
- Exploit Cluster

Risk Prediction



The risk prediction works on the basis of an underlying AI, which is able to predict the exploit probability over a period of time, if the vulnerability is not closed.

The red line shows the estimated risk development. It starts with the proof of concept and a high exploit probability.

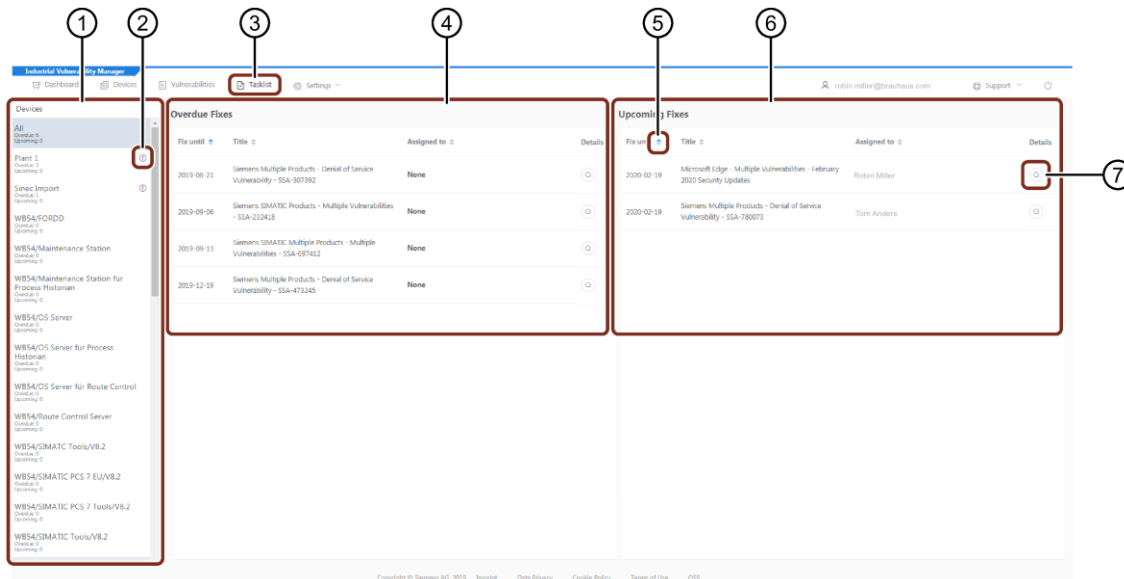
The green area marks the confidence interval over a period of time within a proof of concept and a high exploit probability are expected.

This prediction is based on historical data of vulnerabilities of a similar kind. Even though there is a certain date shown in the prediction, there is no guarantee that a running exploit is only available after the marked period of time.

Note

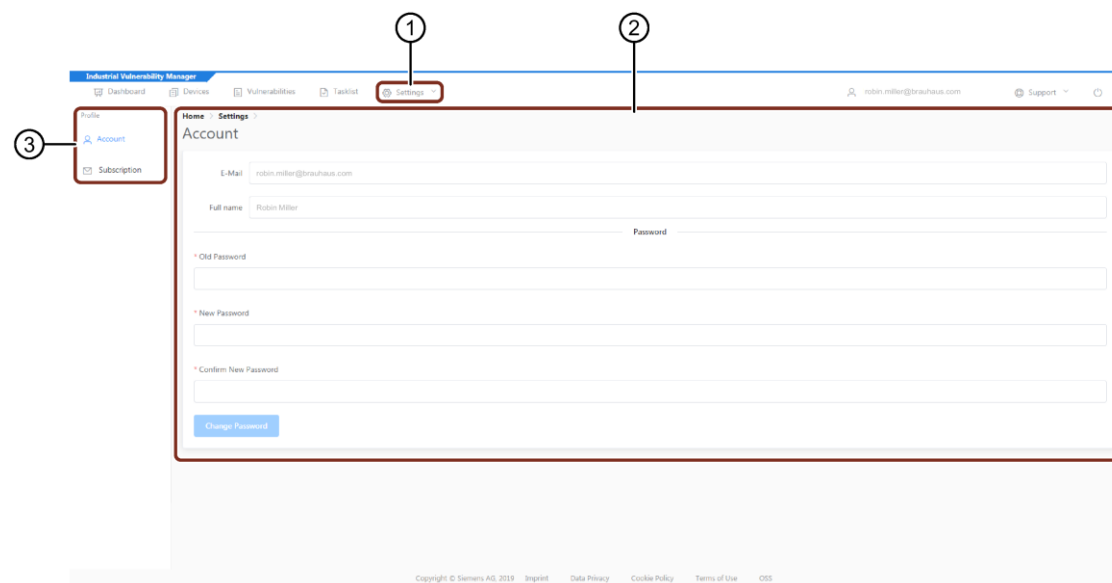
Siemens does not give any guarantee for the correctness of the predicted risk development. Siemens is not responsible for any decisions or consequences arise from the prediction.

2.6 Tasklist User Interface



- ① Device lists
- ② Info field with mouseover function that informs about additional, unassigned vulnerabilities that can be displayed by clicking on the field
- ③ Active tab "Tasklist"
- ④ List of vulnerabilities with processing date in the past
- ⑤ Determine order
- ⑥ List of vulnerabilities with processing date in the future
- ⑦ Go to detail view of the vulnerability

2.7 Settings User Interface



- ① Active tab "Settings"
- ② Input fields of the respective submenu: here "Account"
- ③ Open menu "Profile" > "Account" or "Subscription"

Using the Industrial Vulnerability Manager

3.1 Checking Components for Vulnerabilities

To check a component for vulnerabilities, a component list must be created.

There are 2 ways to create a component list:

- "Creating a New Device or Product and Adding Components Individually (Page 21)"
- "Importing a list with multiple components (Page 24)"

3.1.1 Creating a New List and Adding Components Individually

For components to be assigned to a device or product, a device or product has already been created, or a new device or product is created.

In the following we describe how to create a new device or product and subsequently assign one or several components to this.

3.1.1.1 Creating New List

Example scenario

A user wants to inform himself about possible vulnerabilities of his components.

To do this, a new device or product must first be created. The user can then assign components to this product.

Objective

A new list should be available for selection in the device overview of "Inventory". Components are to be assigned to this product.

Requirement


The "Inventory" tab is open.

3.1 Checking Components for Vulnerabilities

Procedure

To create a new device or product, proceed as follows:

1. Click "+ Add List".
2. Enter the name of the device or product and click "Confirm".



Result

A new device or product has been created and is displayed in the device overview.

3.1.1.2 Adding Individual Components

Example scenario

A user wants to add new components to a lists in order to be informed about possible vulnerabilities.

Objective

A new component is to be added to an existing list in the device overview of "Inventory".

Requirements

- The " Inventory " tab is open.
- The list has already been created.
- The list was selected in the device overview of "Inventory".

Procedure

To add a new component to an existing device or product, proceed as follows:

1. Click "Add component".
2. In the search field, enter the manufacturer and/or the name of the new component, e.g. "Siemens PCS7".

3. A list of recommended components is displayed.
 - If you do not want any search suggestions, click "Skip". This takes you directly to the next input window.
 - If you want the search suggestions, select your component from the list and complete the selection with "Confirm".

The screenshot shows a window titled "Add new Component" with a search bar at the top containing "Siemens PCS 7". Below the search bar is a table with three columns: "Vendor", "Name", and "Version". The table lists several Siemens PCS 7 components, with "PCS7 Advanced Process Library" selected. At the bottom right, there are "Cancel" and "Confirm" buttons.

Vendor	Name	Version
Siemens	OpenPCS 7	8.1
Siemens	OpenPCS 7	8.2
Siemens	OpenPCS 7	9.0 Upd1
Siemens	PCS7 Advanced Process Library	7.1 SP5
Siemens	PCS7 Advanced Process Library	8.0
Siemens	PCS7 Advanced Process Library	8.0 SP1
Siemens	PCS7 Advanced Process Library	8.0 SP2
Siemens	PCS7 Advanced Process Library	8.1
Siemens	PCS7 Advanced Process Library	8.1.2 + Upd2
Siemens	PCS7 Advanced Process Library	8.2

4. A new text input window opens.
 - Check the information about the manufacturer, name and version and change it if needed.
 - Select "Search" to return to the search help with the search suggestions.

The screenshot shows a window titled "Add new Component" with three input fields: "Vendor" (containing "Siemens"), "Name" (containing "PCS7 Advanced Process Library"), and "Version" (containing "7.1 SP5"). At the bottom right, there are "Search", "Cancel", and "Save" buttons.

5. Click "Save" to save the new component.
6. Repeat the steps if you want to add more components.

Result

The created component is displayed in the list overview of "Inventory".
The system checks whether the created component exists and is already monitored.

3.1 Checking Components for Vulnerabilities

The monitoring status is displayed in the components list overview.

Note

If the components are not monitored, contact your PSS Operational Manager to coordinate future monitoring of this component.

3.1.2 Importing a list with multiple components

An already filled file enables you to create one or more new lists that already contain one or more components.

1. From the software you are using export a file that contains a list with several components. The Industrial Vulnerability Manager supports the following software:
 - Standard list/file import
 - Extended list/file import
 - SNMC V8
 - SNMC V9
 - Proneta
 - SIESTA
 - TIA Portal
 - SINEC NMS (Network Management System)
 - WMIC (Windows Management Instrumentation Console)
 - SAS-DC (SIMATIC Assessment Suite - Data Collector)
 - SAS-CR (SMATIC Assessment Suite - Central Report)
2. Import the previously exported file using the Industrial Vulnerability Manager as described in section "Importing a File (Page 25)".

After this file has been successfully imported, the lists and components contained in it are automatically created in the Industrial Vulnerability Manager.

Note

You can create CSV files yourself if you follow certain formatting rules (see Creating a CSV File (Page 26)).

3.1.2.1 Importing a File

Example scenario

A user wants to add a component list with several components to a device.

To do this, the previously exported or created file must be imported into the Industrial Vulnerability Manager.

Objective


All components contained in the previously exported file should be displayed and monitored in the component overview of "Inventory".

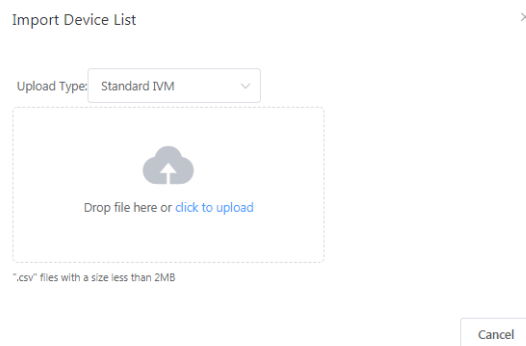
Requirements

- The component list is available as a file in appropriate format (.csv, .xlsx, .json or .aml).
- The "Inventory" tab is open.

Procedure

To import a file, proceed as follows:

1. In the Inventory overview, select the list to which the components are to be assigned.
2. Click "...".
3. Click " Import lists".
4. Select the previously exported or created file.





5. Click "OK".

Extended file import/ Export

Within Version 1.4.0 a new feature was added named Extended file import/export. This function allows to import or export one or several lists including components with their vulnerabilities and individual settings as well as comments.

It can be found under:

3.1 Checking Components for Vulnerabilities

1. In the Inventory overview, select the list to which the components are to be assigned.
2. Click " .
3. Click "  Import Extended File ".
4. Select a previously exported or created file.

Result

All lists with the corresponding components that are contained in the imported file are displayed in the list overview of "Inventory".

The system checks whether the components created exist and are already being monitored.

The monitoring status is displayed in the components list overview.

Note

If the components are not monitored, contact your PSS Operational Manager to coordinate future monitoring of this component.

3.1.2.2 Creating a CSV File

Example scenario

A user wants to add several components to a device or a product.

To do this, components list first has to be created in the form of a CSV file outside of the Industrial Vulnerability Manager application.

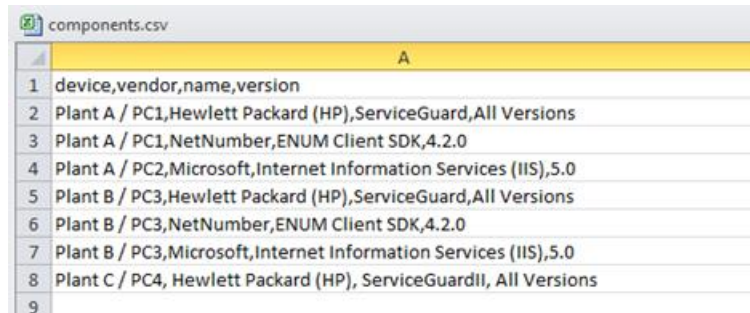
Objective

A CSV file that contains all components needs to be created.

Procedure

To create a CSV file, proceed as follows:

1. Open a program, such as Microsoft Excel, with which you can create a CSV file.
2. Write the name of the list, manufacturer, name and version in a single line separated by a comma for each component.



	A
1	device,vendor,name,version
2	Plant A / PC1,Hewlett Packard (HP),ServiceGuard,All Versions
3	Plant A / PC1,NetNumber,ENUM Client SDK,4.2.0
4	Plant A / PC2,Microsoft,Internet Information Services (IIS),5.0
5	Plant B / PC3,Hewlett Packard (HP),ServiceGuard,All Versions
6	Plant B / PC3,NetNumber,ENUM Client SDK,4.2.0
7	Plant B / PC3,Microsoft,Internet Information Services (IIS),5.0
8	Plant C / PC4, Hewlett Packard (HP), ServiceGuardII, All Versions
9	

Note

Optionally, you have the possibility to insert a separator "/" instead of "," behind the name of the list, to get a hierarchical arrangement of the lists.

3. Save the CSV file.

Result

A CSV file with all lists and the corresponding components is available for upload.

3.1.2.3 Extended File import/ Export function

About

Within Version 1.4.0 a new feature was added named Extended file import/export. This function allows to import or export one or several lists including components with their vulnerabilities and individual settings as well as comments.

Procedure

Extended File import/Export can be found under:

5. In the Inventory overview, select the list to which the components are to be assigned.
6. Click "☰".
7. Click "⬆ Import Extended File " or "⬇ Export Extended File ".

3.2 Assigning a Status to Vulnerabilities

Example scenario

An employee wants to obtain a better overview of the condition or the defined measures for the existing vulnerabilities.

For this purpose a status can be assigned to each vulnerability.

Objective

A status should be assigned to each vulnerability.

Requirement

The "Vulnerabilities" tab is open.

Procedure

There are two ways to assign a status to components:

- **Status assignment in component line or detail view:**

If components are processed individually or in small numbers, the direct path via the component overview or via the detail view is selected.

- **Status assignment using multiple selection:**

If several components are to be assigned a new status at the same time, they are assigned using multiple selection.

Status assignment in component overview under "Inventory" tab or detail view

Status assignment in component overview under "Inventory" tab

To assign a status to a vulnerability directly in the **component overview**, proceed as follows:

1. If needed, search for a vulnerability using the search or filter function.
2. Open the selection menu of the "Status" column.

	Date	Title	Component				Patch Status	Priority	Status	Details
			Vendor	Name	Version	Device				
<input type="checkbox"/>	2019-08-13	Siemens SCALANCE X-200 - Denial of Service Vulnerability - SSA-100232	Siemens	SCALANCE X212-2	All Versions	Sinec Import	Temporary Fix	Major	Analysis Ongoing	
<input type="checkbox"/>	2019-06-11	Siemens SCALANCE X Switches - Information Disclosure Vulnerability - SSA-646841	Siemens	SCALANCE X414-3E	All Versions	Sinec Import	Official Fix	Critical	Open	
<input type="checkbox"/>	2019-06-11	Siemens SCALANCE X Switches - Information Disclosure Vulnerability - SSA-646841	Siemens	SCALANCE X212-2	All Versions	Sinec Import	Official Fix	Critical	Analysis Ongoing	
									Closed	
									Acknowledged	
									Open	

3. Select the status of the vulnerability.
4. Use the same approach for all vulnerabilities.

Status assignment in detail view

To assign a status to a vulnerability directly in the **detail view**, proceed as follows:

1. If needed, search for a vulnerability using the search or filter function.
2. Click "🔍" in the corresponding component line.
3. Select the status of the vulnerability.



4. Use the same approach for all vulnerabilities.

Status assignment using multiple selection

To assign a status to one or more vulnerabilities using multiple selection, proceed as follows:

1. If needed, search for the vulnerabilities using the search or filter function.
2. Place a check mark in front of the desired components and determine the status of the vulnerability.

3 item(s) selected

Status: Select

	Date	Title	Component				Patch Status	Priority	Status	Details
			Vendor	Name	Version	Device				
<input checked="" type="checkbox"/>	2019-08-13	Siemens SCALANCE X-200 - Denial of Service Vulnerability - SSA-100232	Siemens	SCALANCE X212-2	All Versions	Sinac Import	Temporary Fix	Major	Analysis Ongoing	🔍
<input checked="" type="checkbox"/>	2019-06-11	Siemens SCALANCE X Switches - Information Disclosure Vulnerability - SSA-646841	Siemens	SCALANCE X212-2	All Versions	Sinac Import	Official Fix	Critical	Open	🔍
<input checked="" type="checkbox"/>	2019-06-11	Siemens SCALANCE X Switches - Information Disclosure Vulnerability - SSA-646841	Siemens	SCALANCE X414-3E	All Versions	Sinac Import	Official Fix	Critical	Open	🔍

Result


A status is assigned to all vulnerabilities.

3.3 Exporting Monitoring Lists


Components can be exported under the "Inventory" tab. You obtain a Monitoring list as an Excel file.

There are two export options:

- "Export monitored"

All selected components that are monitored are exported. The monitored components are marked with .

- "Export unmonitored"

All selected components that are **not** monitored are exported. The components that are not monitored are marked with .

Example scenario

An employee has discovered that there are components in the bottling plant that have not been checked for vulnerabilities for days. To perform this check, the employee wants to export the component lists of the unmonitored components and forward them to the administrator. The administrator should decide on the next steps.

Objective

The unmonitored components of the bottling plant are to be exported.

Requirement

The "Inventory" tab is open.

Procedure

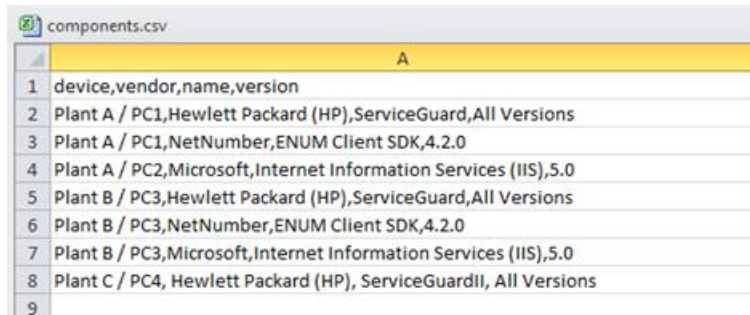
To export a component list with unmonitored components, proceed as follows:

1. In the list overview of "Inventory", select the desired lists.
2. Optionally, use the search field to restrict the component list to a specific component group.
3. Click "... " to open the drop-down menu and click "Export unmonitored".

The file is downloaded. A dialog might open that prompts you to select a target directory for the saving.

Result

The component list has been exported as a CSV file and can be forwarded to the administrator. The administrator can open the CSV file with an external program, such as Microsoft Excel.




	device	vendor	name	version
1	Plant A / PC1	Hewlett Packard (HP)	ServiceGuard	All Versions
2	Plant A / PC1	NetNumber	ENUM Client SDK	4.2.0
3	Plant A / PC2	Microsoft	Internet Information Services (IIS)	5.0
4	Plant B / PC3	Hewlett Packard (HP)	ServiceGuard	All Versions
5	Plant B / PC3	NetNumber	ENUM Client SDK	4.2.0
6	Plant B / PC3	Microsoft	Internet Information Services (IIS)	5.0
7	Plant C / PC4	Hewlett Packard (HP)	ServiceGuardII	All Versions
8				
9				

3.4 Using the Tasklist

All vulnerabilities to which you have assigned a processing date are displayed in the Tasklist.

The vulnerabilities are sorted chronologically and divided into two groups: "Overdue Fixes" and "Upcoming Fixes"

The "Tasklist" tab allows you to switch to the detailed view of the vulnerability:

1. Click .
2. Change or add information about the vulnerability, if necessary:
 - Processing date
 - Status
 - Person to whom the vulnerability was assigned
 - Leave a comment

3.5 Using Dashboard Filter Options

In addition to the two filter options "List" and "Date", filter settings can be made directly in the diagram graphic.

To apply a filter directly in the diagram graphic, click the respective term that is not to be displayed.

Example scenario

An employee creates a risk analysis for his superior. In his risk analysis, he would like to have a tabular representation as well as a graphical representation of all vulnerabilities with the status "Open" and "Analysis Ongoing".

Objective

In addition to a tabular view, the employee also wants a graphical representation of the vulnerabilities with the status "Open" and "Analysis Ongoing".

Requirement

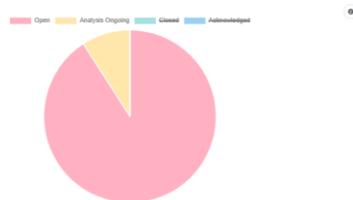
The employee has access to the application and has logged in.

Procedure for graphical view

To get the correct diagram, proceed as follows:

1. Select the desired data in the filter options "List" and "Date".
2. Click the status "Closed" and "Acknowledged" in the "Vulnerability Status" diagram.

Both terms are crossed out and the cleared statuses are not displayed anymore.



Result

Only the vulnerabilities with the status "Open" and "Analysis Ongoing" are displayed in the diagram.

4

Settings

4.1 Profile

The submenus "Account" and "Subscription" are located under the menu "Settings" > "Profile".

4.1.1 Account

In the menu "Account", the User has the possibility to change their password themselves.

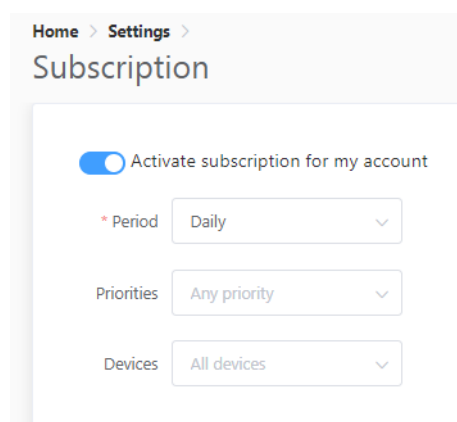
4.1.2 Subscription

The "Subscription" menu allows you to enable email notifications for selected lists.

Note

To use the email notification function, an SMTP server must be stored in the configuration file of the On-Premise version after the installation of the Industrial Vulnerability Manager application.

- In the installation manual of the Industrial Vulnerability Manager, modify the SMTP parameters as described in "Table of environmental parameters".
 - The SMTP_HOST and SMTP_PORT parameters are mandatory for a minimal installation.
-



The screenshot shows the 'Subscription' settings page. At the top, there is a breadcrumb trail: 'Home > Settings > Subscription'. Below this, there is a toggle switch labeled 'Activate subscription for my account' which is currently turned on. Underneath the toggle, there are three dropdown menus: 'Period' set to 'Daily', 'Priorities' set to 'Any priority', and 'Devices' set to 'All devices'.

In the selection menu you can decide for which lists you want to receive notifications and which priorities the notifications should have.

Change History

Version	Date	Change
V1.0.0	10/2018	Release for MindSphere
V1.1.0	09/2019	Manual adapted to new version of Industrial Vulnerability Manager (MindSphere / AWS)
V1.2.0	02/2020	Manual adapted to new version of Industrial Vulnerability Manager (MindSphere / AWS)
V1.2.1	06/2021	Manual language changed to English and adapted to the new version of Industrial Vulnerability Manager (MindSphere / AWS)
V1.4.0	09/2023	New features and naming change included ; Renaming of Devices to Inventory / Lists