

Recording user activity on a SIMATIC Controller using a SIEM System

SIMATIC Controller S7-410-5H, S7-410E
SIMATIC PCS 7

<https://support.industry.siemens.com/cs/ww/en/view/109748211>

Siemens
Industry
Online
Support



Warranty and liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.

If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document. Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply 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 <http://www.siemens.com/industrialsecurity>.

Table of Contents

	Warranty and liability.....	2
1	Task.....	4
2	Solution.....	6
2.1	Overview.....	6
2.2	Hardware and software components	8
2.2.1	Validity	8
2.2.2	Components used	8
2.3	Description of the core functionality for determining the user name.....	10
2.4	Requirements / scenarios.....	11
3	Configuration	14
3.1	Create and provide the configuration files for IP mapping	14
3.2	Configuration of the ES server	15
3.3	Configuration of the CPU 410	16
3.4	Configuration of the SIEM system.....	17
4	Function test	40
5	List of abbreviations.....	42
6	Related literature	43
7	History.....	43

1 Task

Introduction

Modern automation infrastructures are becoming increasingly complex. The individual stations and components in the automation plant are increasingly networked and develop continuously. Due to this deep complexity and networking as well as the standardization, certification and regulatory requirements (including the IT Security Act [\6\](#)), the issue of industrial security is becoming increasingly important.

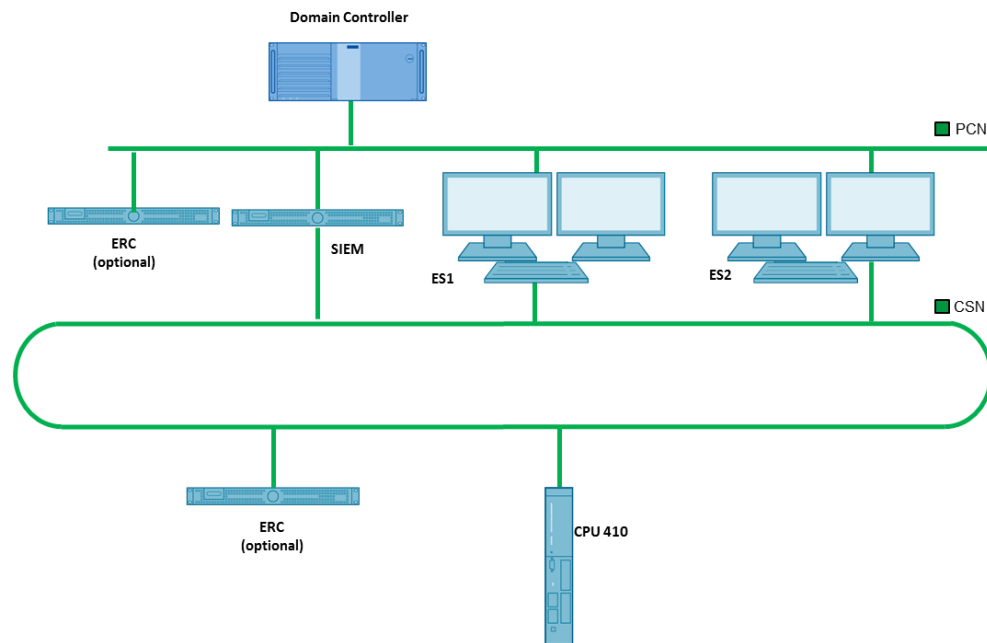
In order to meet the requirements of leading security standard IEC 62443 ([\5\](#)) in the industrial environment, one measure that must be taken is fully recording all user activities. An important prerequisite for this is the generation and provision of appropriate security events. Security events are considered all security-relevant events that are generated in involved system components and sent to the SIEM system or made available for retrieval. Such events are generated by a variety of components (for example, industrial PCs, servers, network components, controllers) and include, among other things, information about the activities performed by different users (for example logins, configuration changes).

SIMATIC controllers (e.g. CPU 410) do not feature user administration, unlike some other systems established in the industrial environment (for example, various operating systems from Microsoft). Such a controller recognizes a legitimate user only when the correct password is entered, which is also referred to as a protection level password. A login shared by several users cannot be resolved to a specific person. Therefore it is not necessary to provide the user name as part of their security events. However, determination of the user name for the individual events of the controller can be implemented using what is referred to as a "Security Information and Event Management System (SIEM)".

Overview of the automation task

The figure below provides an overview of the automation task:

Figure 1-1



Description of the automation task

When using a SIEM system (McAfee SIEM in this case), the task is to record the user activity as completely as possible. In particular, the name of the user who performs certain actions on a SIMATIC controller should be recorded.

However, since login to a SIMATIC controller (e.g. CPU 410) is performed with a valid password and without a user name, this must be determined for the individual logged actions using correlation rules. This is done with the aid of a SIEM system, "McAfee SIEM" in this case.

2 Solution

2.1 Overview

Diagram

The present document describes an approach for applicative determination of the user name using a SIEM system. The approach is also illustrated using the example of the SIEM system by McAfee, McAfee SIEM.

The term "SIMATIC controllers" used in this document refers to the SIMATIC controllers CPU 410-5H and CPU 410E.

The plant diagram according to [Figure 1-1](#) shows the network architecture and the systems involved (highly simplified). The SIEM system (McAfee SIEM in this case) consists of the actual hardware appliance in the plant network, running McAfee ESM, McAfee ELM, and the McAfee ACE correlation engine. The system also has a receiver (ERC) to receive the events of the system components, the SIMATIC controller in this scenario, as well as the engineering stations (ES) from the PCN and CSN network. These systems can be either dedicated or available as a "ComboBox".

Alternatively, ERC dedicated receivers can also be installed in each network (PCN, CSN). The events received by these receivers are subsequently normalized and, if necessary, passed in aggregated form to the higher-level SIEM system.

The engineering stations (ES1 and ES2) belong to a Windows domain. On the domain server responsible for the domain, the user administration is implemented via Microsoft Active Directory (AD).

Each user is clearly identifiable in the network via his own login.

Benefits

The solution presented in this document with the core functionality described in the [Task](#) offers the following advantages:

- It enables efficient applicative determination of the user name and thus improves proactive detection of unauthorized access and deviations from normal behavior, as well as compliance with relevant standardization, certification and regulatory requirements.
- It is based on standard mechanisms of a SIEM system and should therefore be installed on every SIEM system.

Exclusions

This application example does not contain descriptions of the following topics:

- Set up and management of Active Directory entries
- Set up and management of access rights
- System installation and/or configuration
- Network planning and/or configuration
- Plant design
- Configuration of the SIEM system for receiving events of the system components
- Configuration of the engineering stations (ES) for transferring events to the SIEM system

Furthermore, with the correlation rule described in this document, it is only possible to determine the user name from known engineering stations integrated in the SIEM system. Unauthorized access cannot be detected and reported by the SIEM system with the correlation rule described in this application example. This requires further correlation rules, which are not covered in this document.

Required knowledge

Basic knowledge of the SIEM system "McAfee SIEM" and the setup and management of Active Directory entries, as well as Windows user and rights management are required.

2.2 Hardware and software components

2.2.1 Validity

This application example is valid for the following SIMATIC controllers:

- CPU 410-5H, as of Firmware V8.2.0
- CPU 410E, as of Firmware V8.2.0

as well as for the following SIEM system:

- McAfee SIEM (ESM, ELM, ACE, ERC); Version 9.6.0

as well as for the process control system PCS 7 V9.0.

2.2.2 Components used

This application example was tested with the following components:

Hardware components

Component	Article number	HW version	FW version
CPU 410-5H	6ES7 410-5HX08-0AB0	as of V1.0	as of V8.2.0
CPU 410E	6ES7 410-5HM08-0AB0	as of V1.0	as of V8.2.0

Software components

Component	Qty.	Article number	Note
McAfee SIEM	1	External supplier	V9.6.0 MR 9
McAfee ACE	1	External supplier	V9.6.0 MR 9
McAfee ERC*	1*	External supplier	V9.6.0 MR 9
McAfee Windows SIEM Collector	opt	External supplier	V11.0
SIMATIC PCS 7	1	6ES7658-...58-....	V9.0

* One receiver (ERC) may be required per network segment depending on the network and security policies to be fulfilled

A combination system (ComboBox) can also be used as an alternative to dedicated SIEM components (ESM, ELM, ACE, ERC).

Component	Qty.	Article number	Note
McAfee ComboBox ENMELM-4600	1	External supplier	ESM V9.6.0 MR 9
McAfee Windows SIEM Collector	opt	External supplier	V11.0
SIMATIC PCS 7	1	6ES7658-...58-....	V9.0

Example files and projects

The following list contains all the files and projects used in this example.

Component	Note
Correlation_Rule.zip	This file contains the correlation rules to be created
109748211_Recording _user_activity_en.pdf	This document

2.3 Description of the core functionality for determining the user name

Description of system processes

Using the core functionality described in this chapter, the user name is determined by application.

The corresponding correlation rule is based on an implicitly predetermined sequence of events, which are made available to the SIEM system by the components involved.

Access to a SIMATIC controller is usually made from an engineering station (ES) connected in the PCN via a configuration tool such as PCS 7 HW Config. The project engineer logs on to this system with his personal Windows login for this purpose. The user's successful login is recorded in the event memory of the Microsoft Windows operating system, which is called the Windows Event Log. The SIEM system is configured to access and retrieve the events via the WMI (Windows Management Instrumentation) interface. It is recommended that you assign the SIEM system a separate account in the domain and grant this account administrative or explicit access rights. Alternatively, the "Windows SIEM Collector" can be installed on the respective Windows systems and configured so that the corresponding events are forwarded to the SIEM system.

The events are further interpreted and processed by the SIEM system based on the system configuration.

If a change is made to the system configuration on the SIMATIC controller, the events triggered by this action are sent to the SIEM system if the controller has been configured accordingly.

Provided the IP address from which access to the SIMATIC controller is made matches the IP address of the ES, the user name can be extracted from the login events of the Windows system stored in the Windows Event Log.

Note the following in this regard:

Due to network segmentation, the IP address in the PCN network is specified in the login event of the ES. However, the SIMATIC controller is accessed via its IP address in the CSN network. To correctly identify the user name, the IP addresses associated with an ES must be assigned. The "data enrichment" of the SIEM system, McAfee SIEM in this case, is used for this.

The underlying configuration file, which handles the assignment of IP addresses between the PCN and the CSN network, must be created and maintained. A complete and consistent dataset is essential to ensure that the SIEM system draws the right conclusions and that the logged user activities are not corrupted.

Since the user name is to be logged for all configuration changes of an SIMATIC controller, it is recommended to determine the user name for the following events supported by the SIMATIC controller:

Event	Meaning
SE_NETWORK_SUCCESSFUL_LOGON	Correct entry of the protection levels password
SE_ACCESS_PWD_CHANGED	Load configuration with password
SE_SECURITY_CONFIGURATION_CHANGED	Change protection level; Syslog server configuration new/changed
SE_OPMOD_CHANGED	Operating state changed
SE_CFG_DATA_CHANGED	The system configuration of the SIMATIC controller has been changed
SE_USER_PROGRAM_CHANGED	A new user program has been loaded
SE_FIRMWARE_LOADED	Firmware loaded
SE_FIRMWARE_ACTIVATED	Firmware enabled
SE_SYSTEMTIME_CHANGED	System clock time set

A complete description of the events supported by the SIMATIC controller is documented in [4](#).

2.4 Requirements / scenarios

To ensure that the name of the user who performs a specific action on a SIMATIC controller can be determined using the appropriate correlation rules, the following boundary conditions regarding the application environment must be fulfilled:

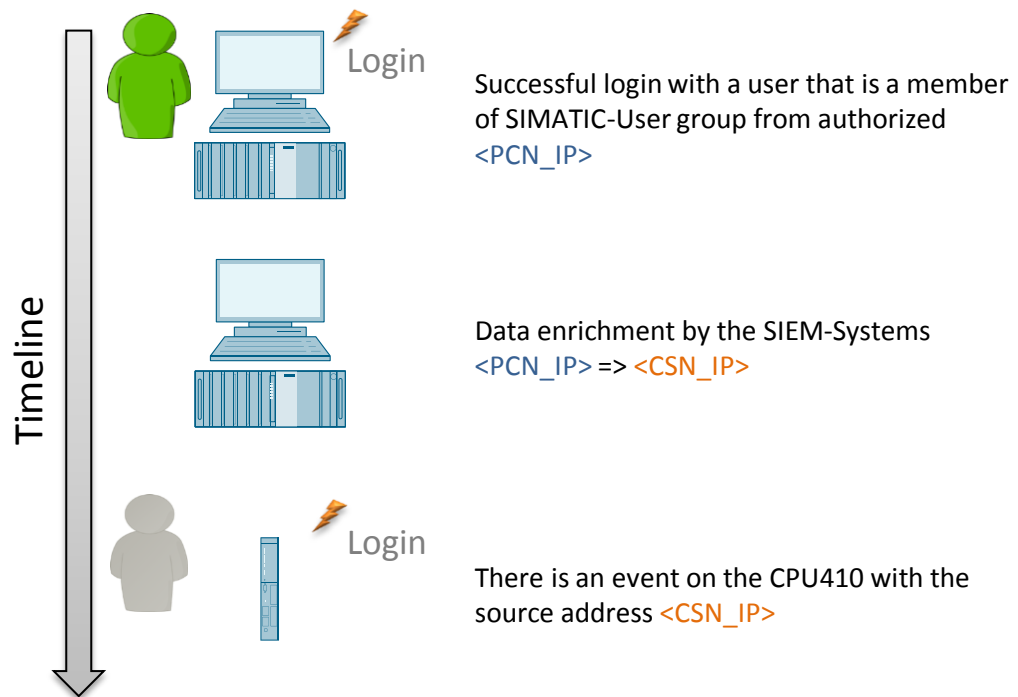
- A previous analysis must be performed to ensure that the available network bandwidth is sufficient for the additional network load
- All involved components (see [Figure 1-1](#)) report the events required for the correlation to the SIEM system or provide them via a defined interface. In this example, the SIMATIC controller reports its events to the SIEM system via the SYSLOG log. The events of the engineering stations are retrieved from the SIEM system via the Microsoft Windows-specific Windows Management Instrumentation (WMI) interface or transferred to the SIEM system via "Windows SIEM Collector".
- All systems involved have a static IP address or are assigned the same IP address by dynamic address assignment (DHCP).
- The identification of the user name relies on the user administration of the automation system. A login shared by several users cannot be resolved to a specific person.
- Only one user can be logged on at a given time on an ES (Single User Mode).
- If the SIEM system retrieves the Windows Event Logs from the system's WMI interface, it is recommended to create a separate account with explicit access rights for the SIEM system.

Note

With the correlation rule described in this document, only user names can be identified by the ES integrated in the SIEM system. If access is performed by a source that is unknown to the SIEM system, neither a user name nor an alarm can be determined by the SIEM system using this correlation rule. This requires additional correlation rules, which are not covered in this document.

Core functionality process

The following figure shows the process of core functionality:



=> Determination of the user name from the login event of the ES with the enriched IP address **<CSN_IP>**

The correlation rule is based on the logical relationships described in the following table.

	Action	Note
1	A user logs on to an ES with a user name.	
2	The associated login event from Windows is sent to the SIEM system via SIEM Collector, or retrieved from the SIEM system via the WMI interface.	If the events are retrieved from the SIEM system from the engineering stations via the WMI interface, it is recommended to configure a separate Windows login.
3	This system accesses the SIMATIC controller and changes the configuration within a defined time window.	The time window is set in the correlation rule and must include at least the work time of the plant operators.
4	The SIMATIC controller sends the events associated with the user action to the SIEM system.	The IP address and port of the SIEM system must have been made known to the SIMATIC controller beforehand.

	Action	Note
		The SIEM system must be accessible to the SIMATIC controller.

With data enrichment, the SIEM system adds the CSN IP address of the system to the login/logout events of the ES as a new parameter. The assignment of the CSN IP address to a PCN IP address is based on a configuration file, which is created, maintained and made available to the SIEM system by the user.

3 Configuration

Note

Configuration is performed in three main steps:

- Create and deploy configuration files
- Configuration of the systems involved to provide the required events
- Configuration of the SIEM system and creation of new correlation rules

3.1 Create and provide the configuration files for IP mapping

PCN – CSN IP addresses

As described in the Task, an ES has two physical interfaces to the PCN or CSN network, while a user logs on via the PCN network and accesses the CPU 410 via the CSN network. The table below provides a step-by-step description for creating a configuration file which is used to map the IP address from PCN to CSN.

No.	Action
1	On your system, create an ASCII text file in any directory with any filename, without special characters, umlauts, or spaces, and set ".txt" as the extension for the file.
2	Open the file in an editor of your choice.
3	Enter an assignment for each line. The PCN-CSN mapping is performed according to the following structure: <PCN_IP>=<CSN_IP> <PCN_IP> is the IP address of the machine in the PCN network, and <CSN_IP> is the IP address of the same machine in the CSN network. Example: 192.168.10.11=192.168.100.1 192.168.10.12=192.168.100.2
4	Save the file.
5	Ensure that the SIEM system can access the file over the network.

In the current version 9.6.0, the SIEM system "McAfee SIEM" supports the following methods for retrieving a file from an external data source (see the documentation [\[7\]](#)):

- CIFS
- FTP
- SCP
- SFTP
- NFS
- http or https

3.2 Configuration of the ES server


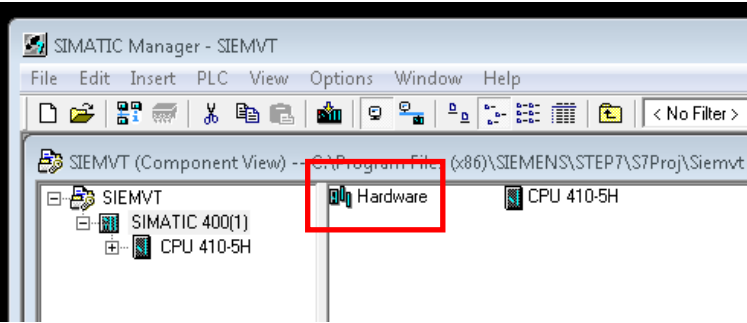
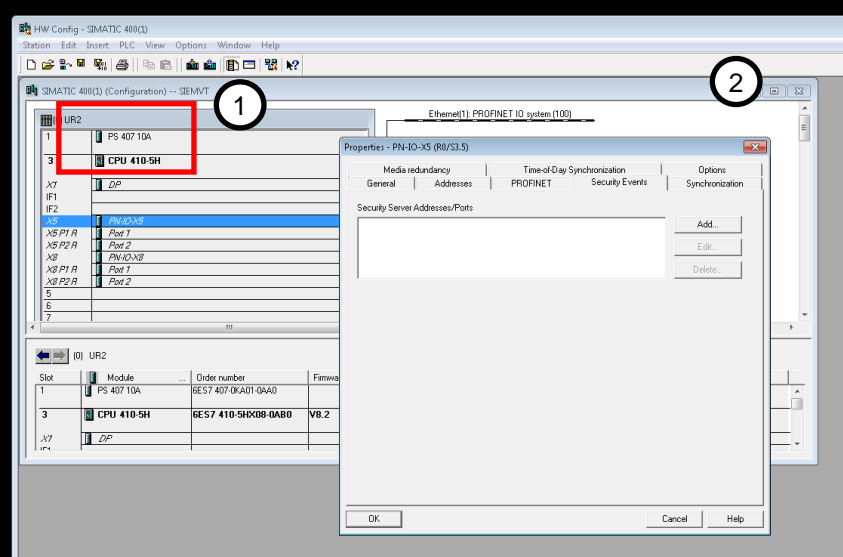
You can learn how to form the Microsoft Windows Event Log in [\8\](#). The following events must be logged by the Windows computer and provided to the SIEM system via WMI in order to correctly perform all the required corrections:

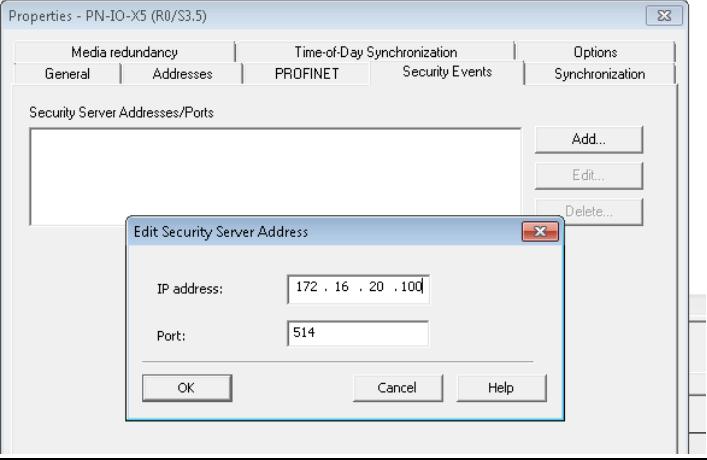
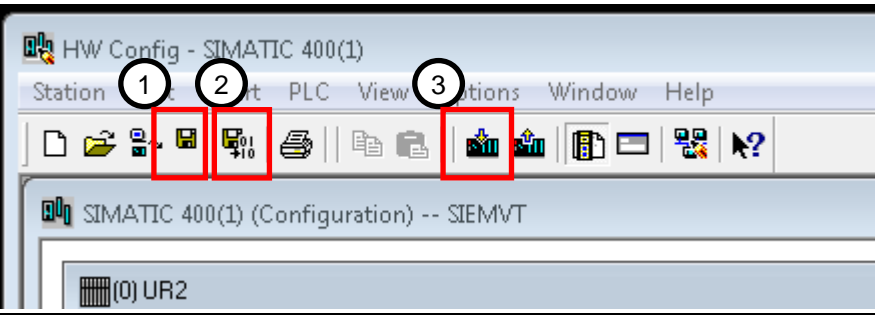
- Account login:
 - Monitor verification of login information
 - Monitor Kerberos Authentication Service
 - Monitor other account login events
- Account management:
 - Monitor computer account management
 - Monitor user account management
- Login/logout:
 - Monitor login
 - Monitor logout
 - Monitor other login/logout events
 - Monitor special login
 - Monitor account lockout

More information on the events mentioned here is provided in [\6\](#).

In [\7\](#), you can find a tutorial on how the Microsoft Windows Event Log can be integrated into the SIEM system via WMI.

3.3 Configuration of the CPU 410

No.	Action
1	Log in to an ES with your user name and valid password.
2	Open your PCS 7 project in the SIMATIC Manager. 
3	Navigate to the configured SIMATIC 400 station and open the hardware configuration 
4	Open the properties of the Ethernet interface through which the SIEM system can be accessed (PN-IO-X5 modules (1) in this case) and switch to the "Security Events" tab (2) 
5	Click on the "Add" button and enter the IP configuration of the SIEM system in the new form.

No.	Action
	
6	Check your entry and then click "OK".
7	Apply your configuration changes by clicking "OK" in the Properties window.
8	<p>Save the project (1) and compile it again (2). Then, load it to the module (3).</p> 
9	Follow the instructions of the wizard to program the modules.
10	Ensure that the module is in the desired operating mode (RUN mode, STOP mode).

3.4 Configuration of the SIEM system

Requirements

- You need sufficient authorizations to create new "Custom types", "Data enrichment", and "Correlation rules".
- The systems (ES, SIMATIC S7-410) required for determining the user name must be successfully created as a data source in the SIEM system.
- The SIEM system must be able to access a data store on the network, which contains the necessary configuration file for IP address mapping.

Note

All details refer to the English user interface.

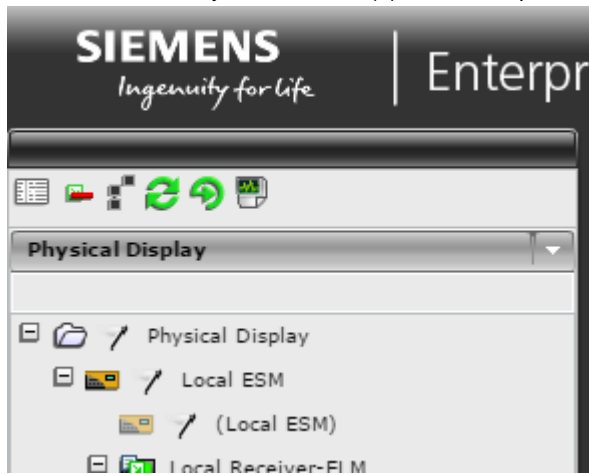
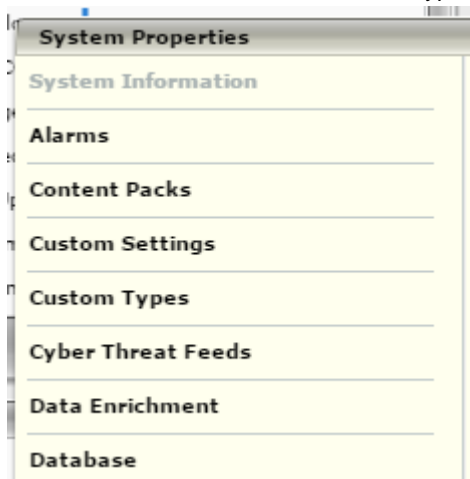
Since the GUI of the ESM can be individually adapted, deviations in the display cannot be ruled out.


Create a new custom type to assign the CSN IP address

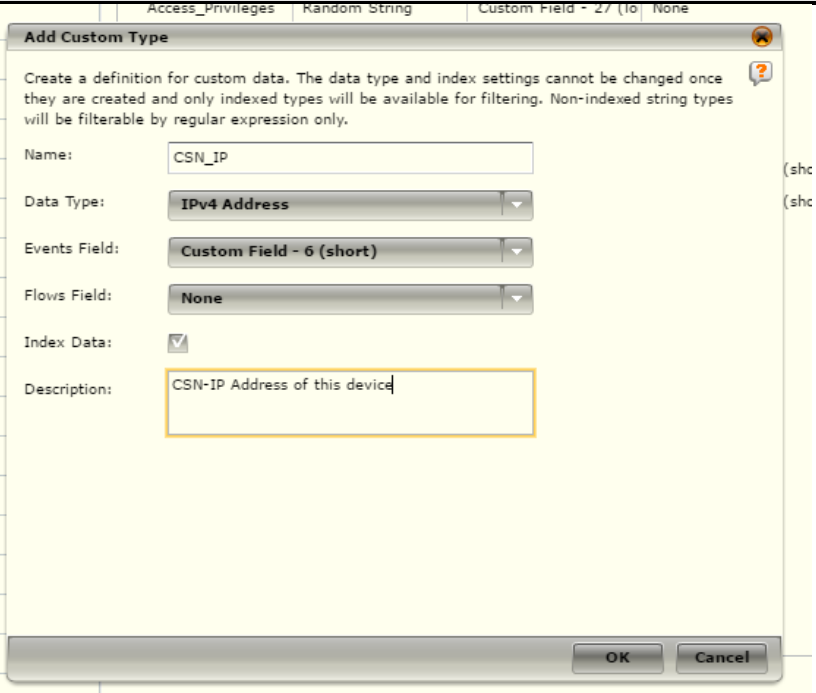
This section describes how to create a custom field for assigning the CSN IP address.

First, check which custom field is available for the new type. To do this, perform steps 1-6 from the description "Extend the field assignment of the parsing rule for the SIMATIC controller" and note the name of an offered type. Take the field assigned for this type from the table of custom types ([step 4](#)).

Table 3-1

No.	Action
1.	Open the web-based user interface for McAfee ESM.
2.	Log in with your user name and the password.
3.	First select the entry "Local ESM" (1) and then open its system properties (2): 
4.	Select the menu command "Custom Types". 
5.	Click on the "Add" to create a custom type.

No.	Action												
	 <p>The following input dialog opens:</p> <p>Add Custom Type</p> <p>Create a definition for custom data. The data type and index settings cannot be changed once they are created and only indexed types will be available for filtering. Non-indexed string types will be filterable by regular expression only.</p> <p>Name: <input type="text"/></p> <p>Data Type: Random String</p> <p>Events Field: None</p> <p>Flows Field: None</p> <p>Index Data: <input checked="" type="checkbox"/></p> <p>Description: <input type="text"/></p> <p>The String data type should be used for strings that appear frequently, such as a user name. Random string should be used if the data appears to be random or does not frequently repeat, such as full URLs. Random strings will not be able to use the Alias or case insensitive options while filtering. Too many entries in a string type may cause a decrease in performance on the ESM. Please select the appropriate string type for the intended use.</p> <p>OK Cancel</p> <p>CSN-IP Address of this device</p>												
6.	<p>Configure the new custom type as follows:</p> <table> <tr> <td>"Name"</td> <td>= "CSN_IP"</td> </tr> <tr> <td>"Data type"</td> <td>= "IPv4 address"</td> </tr> <tr> <td>"Event field"</td> <td>= A free field on your system here: "Custom Field: 6 (short)"</td> </tr> <tr> <td>"Flow Field"</td> <td>= "None"</td> </tr> <tr> <td>"Data Index"</td> <td>= Set checkmark to select</td> </tr> <tr> <td>"Descriptions"</td> <td>= Your description here: "CSN-IP address of this component"</td> </tr> </table>	"Name"	= "CSN_IP"	"Data type"	= "IPv4 address"	"Event field"	= A free field on your system here: "Custom Field: 6 (short)"	"Flow Field"	= "None"	"Data Index"	= Set checkmark to select	"Descriptions"	= Your description here: "CSN-IP address of this component"
"Name"	= "CSN_IP"												
"Data type"	= "IPv4 address"												
"Event field"	= A free field on your system here: "Custom Field: 6 (short)"												
"Flow Field"	= "None"												
"Data Index"	= Set checkmark to select												
"Descriptions"	= Your description here: "CSN-IP address of this component"												

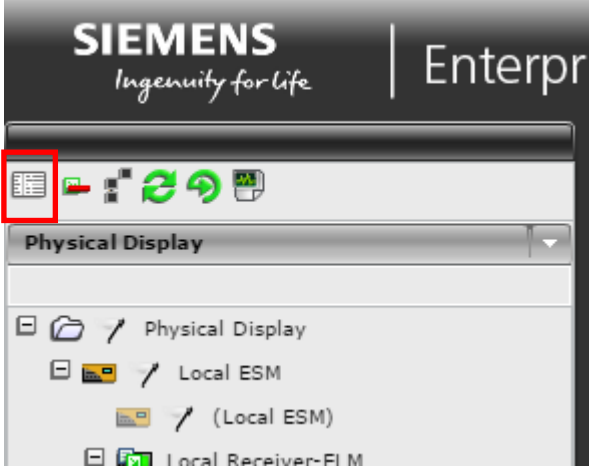
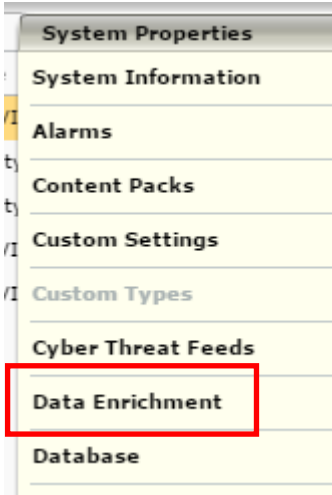
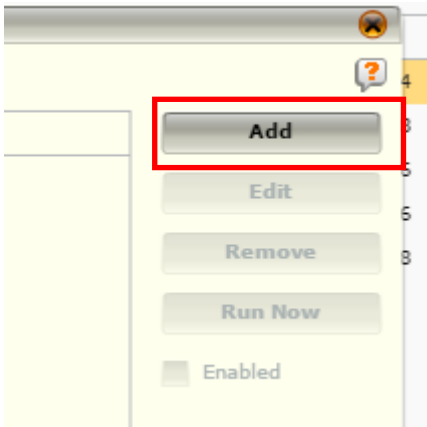
No.	Action
	
7.	Save this setting by clicking the "OK" button.
8.	If you want to proceed directly to the next step of data enrichment, go to step 4 of Table 3-2 .

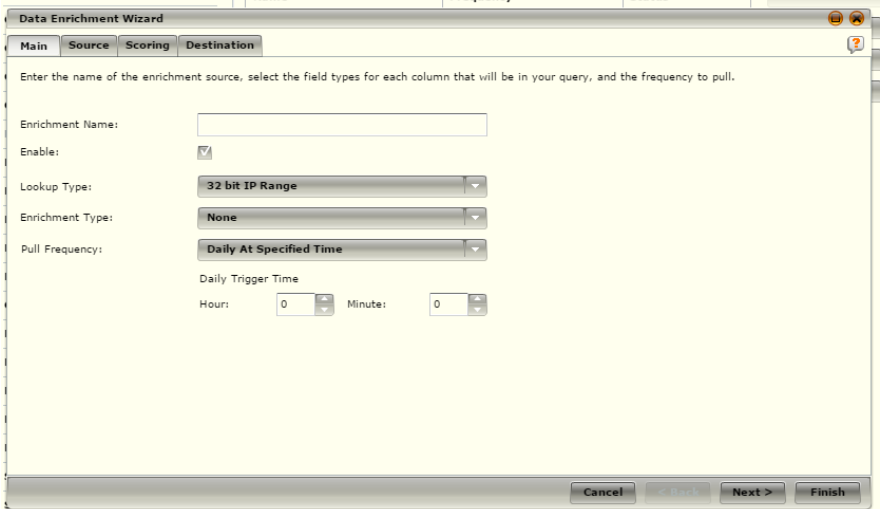
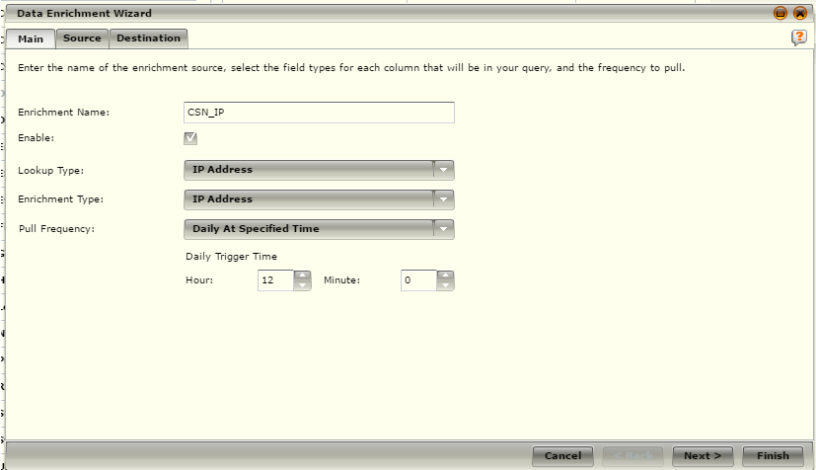
Setting up data enrichment

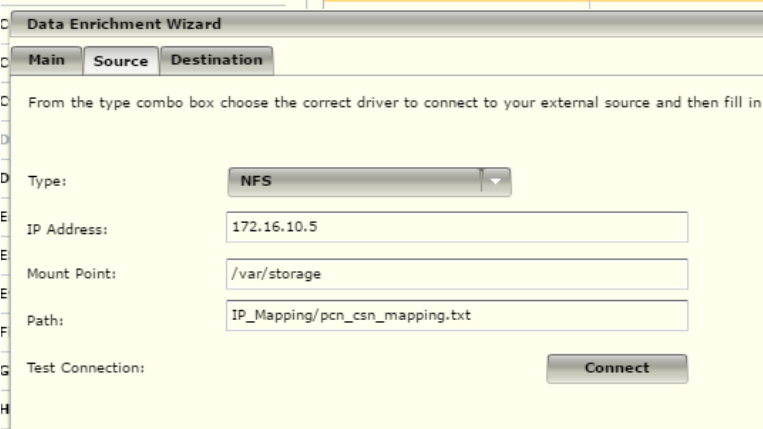
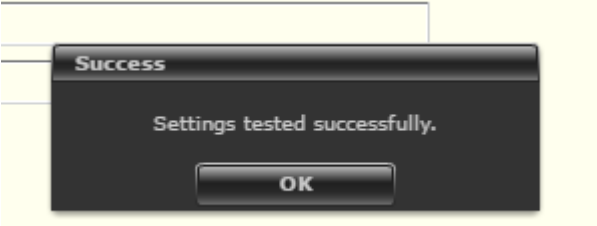
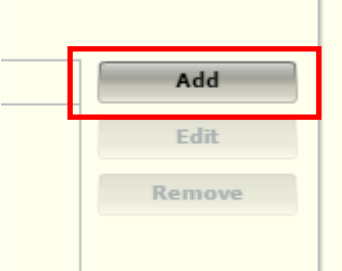
Note The configuration file (see [Table 3-1](#)) must be created and available for opening by the SIEM system.

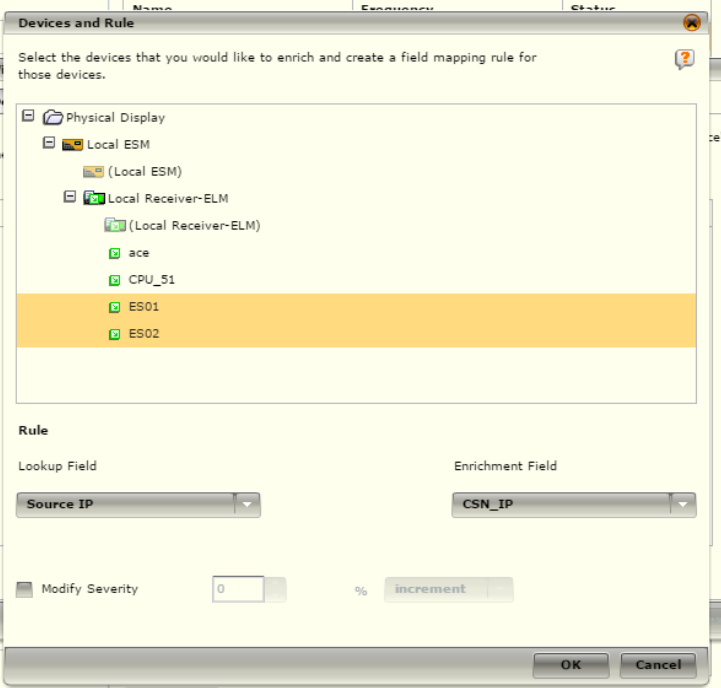
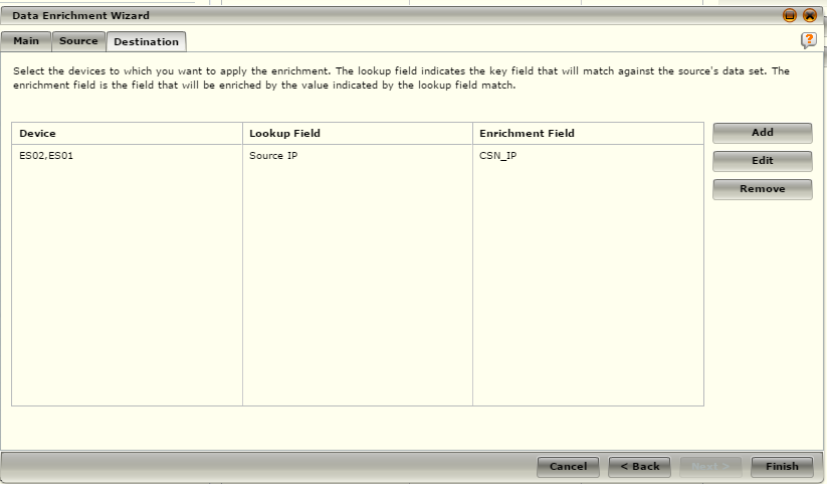
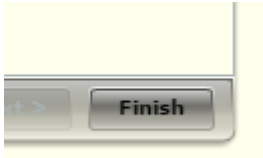
Table 3-2

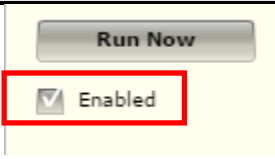
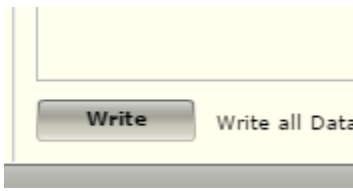
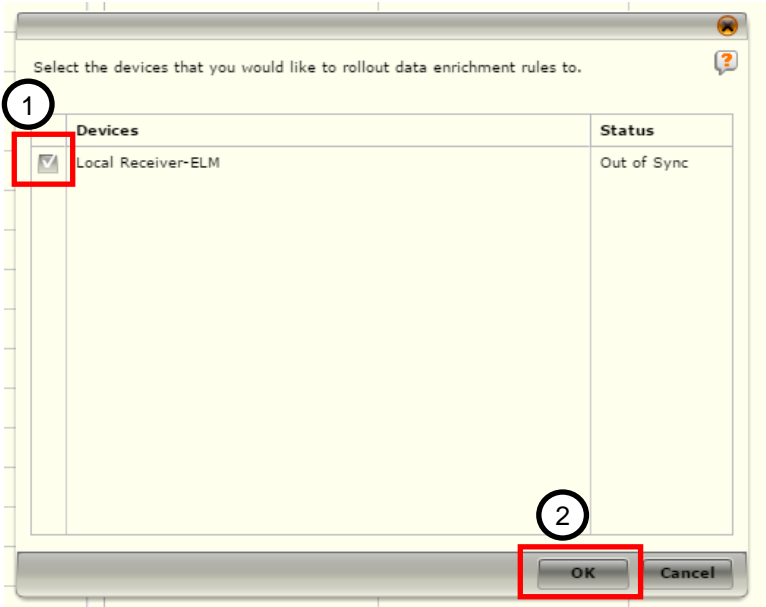
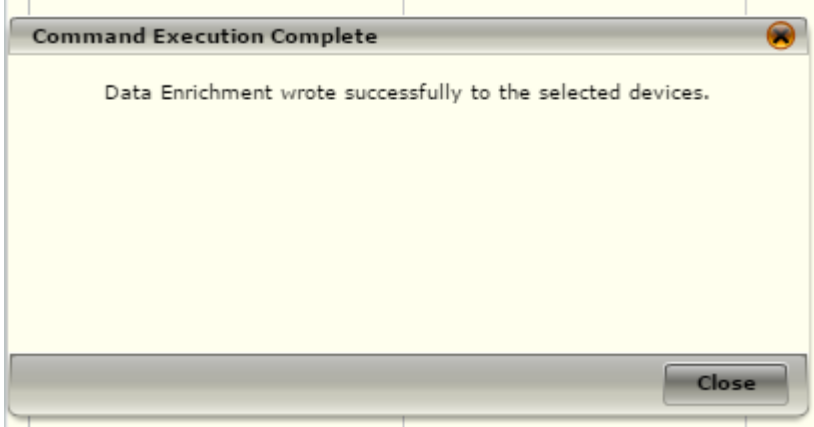
No.	Action
1.	Open the web-based user interface for McAfee SIEM.
2.	Log in with your user name and the password.
3.	Open the system properties of "McAfee SIEM".

No.	Action
	
4.	<p>Select the menu command "Data Enrichment".</p> 
5.	<p>Click on the "Add" button.</p>  <p>The following configuration window opens:</p>

No.	Action
	
6.	<p>Make the following settings in the "Main" tab:</p> <p>"Name" = "CSN_IP"</p> <p>"Enable" = Select by setting a checkmark</p> <p>"Lookup Type" = "IP address"</p> <p>Note: If you select the "IP Address" lookup type of the "Scoring" tab of the configuration window is hidden.</p> <p>"Enrichment Type" = "IP address"</p> <p>"Pull Frequency": = Set how often the SIEM system should read the configuration file again. Since the IP addresses are fixed, a slow update frequency is sufficient, for example: On every first day of a month at 12 noon.</p> 
7.	<p>In the "Source" tab, set the file enable to provide the configuration file for the IP mapping (see chapter 3.1) for the SIEM system.</p>

No.	Action
	
8.	<p>To test the connection configuration, click the "Connect" button. If the connection can be established, the following message is displayed. Check and correct the connection configuration if an error message occurs and test again.</p> 
9.	<p>In the "Destination" tab, click on the "Add" button</p> 
10.	<p>In the newly displayed "Devices and Rule" configuration window, select the affected engineering stations (ES) in the system tree. For a multiple selection, hold down the "Ctrl" key at the same time. In addition, make the following settings in the configuration window: "Lookup field" = "Source IP" "Enrichment Field" = The newly created custom field; "CSN_IP" in this case</p>

No.	Action
	 <p>Note: Alternatively, you can create each ES individually. To do this, click the "Add" button again and make the same settings.</p> <p>After you have added the engineering stations, the input dialog appears as follows:</p> 
11.	<p>Click on the "Finish" button to conclude the configuration.</p> 
12.	<p>Ensure a checkmark is set for the "Enabled" option.</p>

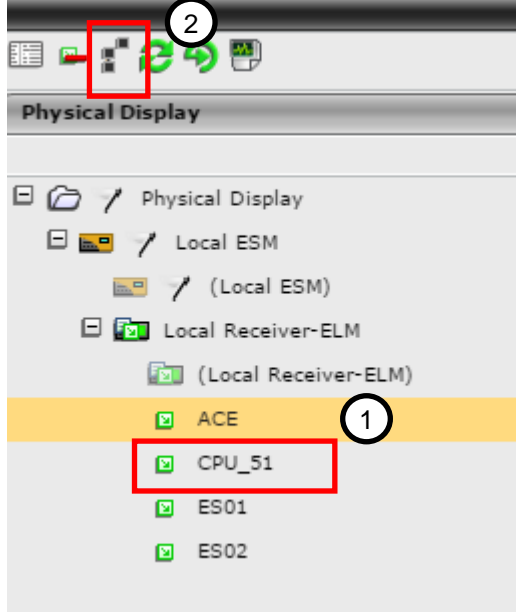
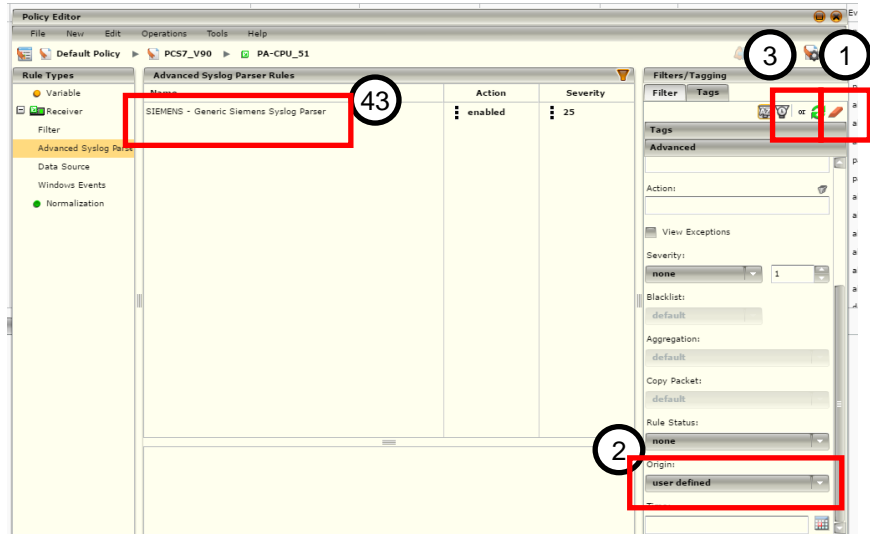
No.	Action
	
13.	<p>Click on the "Write" button to save the settings.</p> 
14.	<p>Select the non-synchronized devices (in this example, Local Receiver-ELM). To start the rollout, click "OK".</p> 
15.	<p>If the data enrichment rules was successfully written, the following dialog is displayed. Close the dialog with the "Close" button.</p> 
16.	<p>Select the created rule "CSN_IP" and click the "Run Now" button. to force a first-time retrieval of the configuration file. Ensure a checkmark is set for the "Enabled" option.</p>

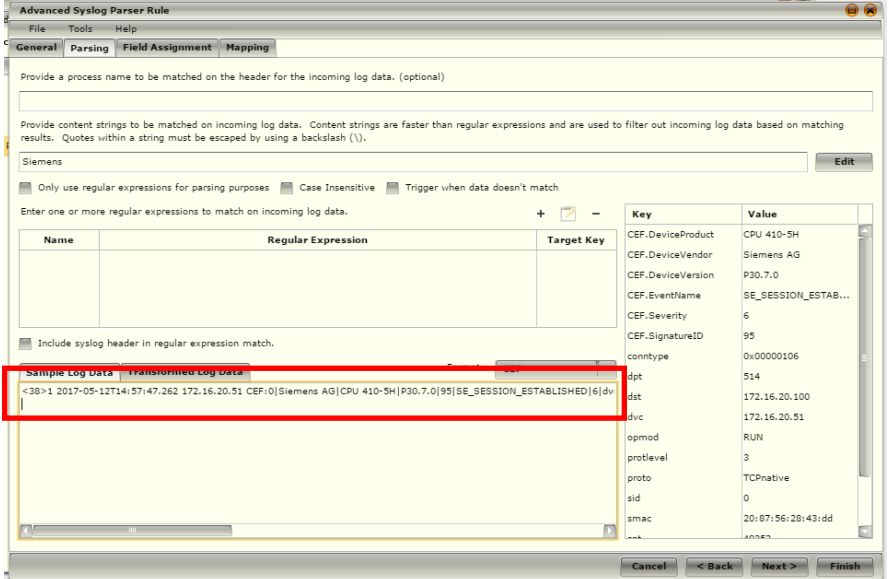
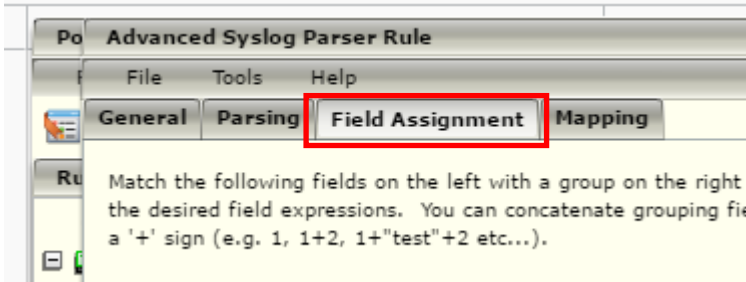
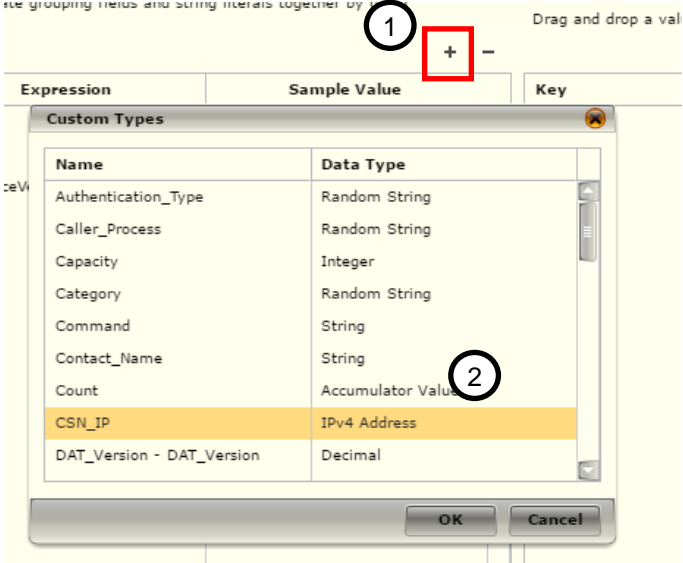
No.	Action									
	<div><p>Click the add button to add a Data Enrichment source.</p><table><thead><tr><th>Name</th><th>Frequency</th><th>Status</th></tr></thead><tbody><tr><td>CSN_IP</td><td>Daily 12 Hr 0 Mins</td><td>Enabled</td></tr><tr><td></td><td></td><td></td></tr></tbody></table><div><p>Add</p><p>Edit</p><p>Remove</p><p>Run Now</p></div></div>	Name	Frequency	Status	CSN_IP	Daily 12 Hr 0 Mins	Enabled			
Name	Frequency	Status								
CSN_IP	Daily 12 Hr 0 Mins	Enabled								
17.	<p>If all settings are correct and the configuration file has been successfully read, the following dialog is displayed. Close this by clicking on the "Close" button.</p> <div><div>Command Execution Complete</div><div>Data Enrichment wrote successfully to the selected devices.</div><div>Close</div></div> <p>The status of the created rule changes from "Enabled" to "<n>" rows processed, where <n> must match the number of IP assignments created in the mapping file created under 3.1.</p> <table><thead><tr><th>Status</th></tr></thead><tbody><tr><td>2 rows processed</td></tr></tbody></table>	Status	2 rows processed							
Status										
2 rows processed										
18.	Force another rollout of the imported mapping file repeating steps 13-15.									

Extend the field assignment of the parsing rule for the SIMATIC controller

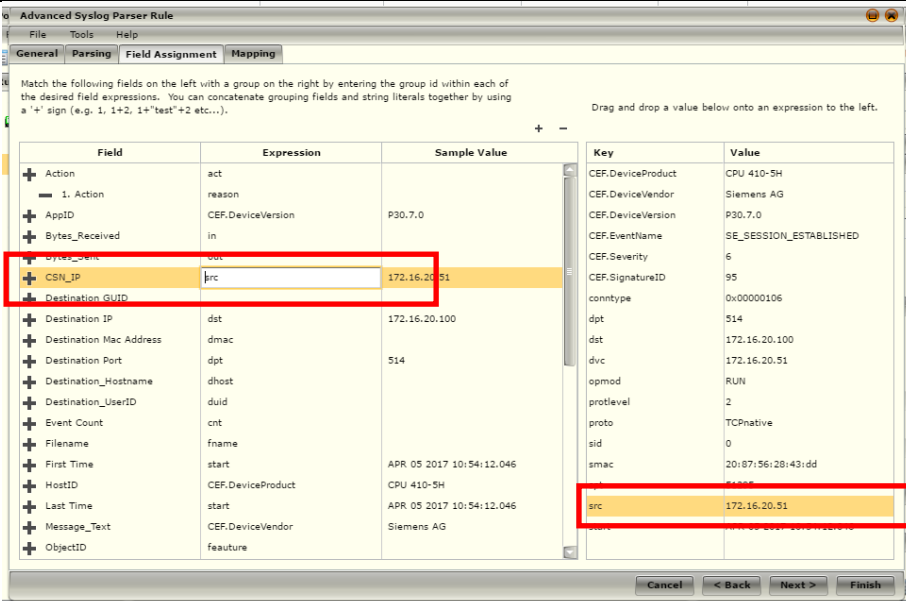
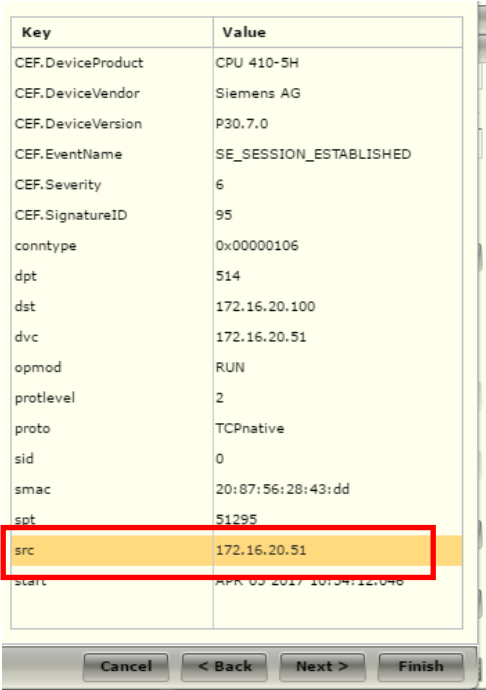
Note The new Custom Field for the IP address of the systems in the CSN Field must be successfully created and available for mapping.

No.	Action
1	Open the web-based user interface for McAfee ESM.
2	Log in with your user name and the password.
3	Open the Policy Editor (2) of the SIMATIC Controller ("CPU_51" in this case) (1).

No.	Action
	
4	<p>Open the corresponding rule for the SIMATIC controller ("SIEMENS - Generic Siemens Syslog Parser" in this case).</p> <p>If needed, adapt the filter on the right side of the Policy Editor to make the search easier. To do this, clear the automatically set filters (1) and select the "Custom" option under "Origin". Refresh the view (3) and select the specified rule (4).</p> 
5	<p>Go to the "Parsing" tab and enter the following event as an example:</p> <pre><38>1 2017-04-05T10:54:12.047 172.16.20.51 CEF:0 Siemens AG CPU 410-5H V8.2.0 95 SE_SESSION_ESTABLISHED 6 dvc=172.16.20.51 protlevel=2 start=APR 05 2017 10:54:12.046 opmod=RUN conntype=0x00000106 sid=0 proto=TCPnative src=172.16.20.51 smac=20:87:56:28:43:dd spt=51295 dst=172.16.20.100 dpt=514</pre>

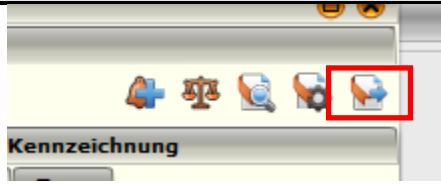
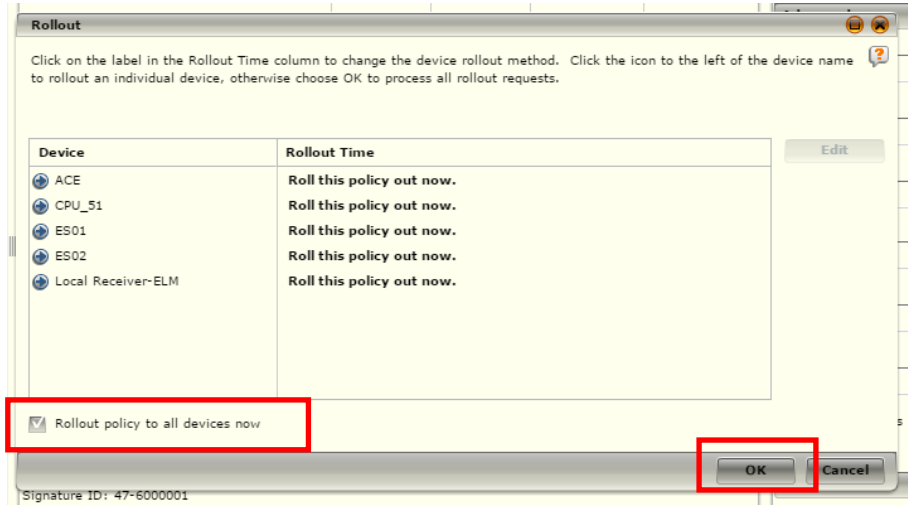
No.	Action
	
6	<p>Go to the "Field Assignment" tab.</p> 
7	<p>Add the new custom field, CSN_IP (2) in this case, created in Table 3-1. To do this, first click on the "+" symbol (1).</p>  <p>Confirm the selection and close the window with the "OK" button.</p>
8	<p>For the "expression", enter the key "src".</p>

3 Configuration

No.	Action
	 <p>OR: In the key table, select the source IP (CEF key: src) and assign it to the "CSN_IP" field using Drag&Drop</p> <p>Note: The parsed keys are only displayed if an example event is displayed in the "Parsing" tab.</p> 
9	Drag&Drop the "src" key into the "CSN_IP" field.

3 Configuration

No.	Action																																																																																															
	<div><div><div><div><div>Advanced Syslog Parser Rule</div><div>File Tools Help</div><div>General Parsing Field Assignment Mapping</div><div>Match the following fields on the left with a group on the right by entering the group id within each of the desired field expressions. You can concatenate grouping fields and string literals together by using a "+" sign (e.g. 1. 1+2. 1="test"+2 etc...).</div><div>Drag and drop a value below onto an expression to the left.</div><div><table><thead><tr><th>Field</th><th>Expression</th><th>Sample Value</th><th>Key</th><th>Value</th></tr></thead><tbody><tr><td>1. Action</td><td>act</td><td></td><td>CEF.DeviceProduct</td><td>CPU 410-5H</td></tr><tr><td>AppID</td><td>CEF.EventName</td><td>SE_SESSION_ESTABLISHED</td><td>CEF.DeviceVendor</td><td>Siemens AG</td></tr><tr><td>Bytes_Received</td><td>CEF.DeviceVersion</td><td>P30.7.0</td><td>CEF.DeviceVersion</td><td>P30.7.0</td></tr><tr><td>Bytes_Sent</td><td>in</td><td></td><td>CEF.EventName</td><td>SE_SESSION_ESTABLISHED</td></tr><tr><td>CSN_IP</td><td>out</td><td></td><td>CEF.Severity</td><td>6</td></tr><tr><td>Destination GUID</td><td>src</td><td>172.16.20.51</td><td>CEF.SignatureID</td><td>95</td></tr><tr><td>Destination IP</td><td>dst</td><td>172.16.20.100</td><td>connType</td><td>0x00000106</td></tr><tr><td>Destination Mac Address</td><td>dmac</td><td></td><td>dpt</td><td>514</td></tr><tr><td>Destination Port</td><td>dpt</td><td>514</td><td>dst</td><td>172.16.20.100</td></tr><tr><td>Destination_Hostname</td><td>dhost</td><td></td><td>dvc</td><td>172.16.20.51</td></tr><tr><td>Destination_UserID</td><td>duid</td><td></td><td>opmod</td><td>RUN</td></tr><tr><td>Event Count</td><td>cnt</td><td></td><td>protlevel</td><td>3</td></tr><tr><td>Filename</td><td>fname</td><td></td><td>proto</td><td>TCPnative</td></tr><tr><td>First Time</td><td>start</td><td>MAY 12 2017 14:57:47.262</td><td>pid</td><td>0</td></tr><tr><td>HostID</td><td>CEF.DeviceProduct</td><td>CPU 410-5H</td><td>smac</td><td>20:07:56:28:43:dd</td></tr><tr><td>Last Time</td><td>start</td><td>MAY 12 2017 14:57:47.262</td><td>spt</td><td>49252</td></tr><tr><td>Message_Text</td><td>CEF.DeviceVendor</td><td>Siemens AG</td><td>src</td><td>172.16.20.51</td></tr><tr><td>ObjectID</td><td>feature</td><td></td><td>start</td><td>MAY 12 2017 14:57:47.262</td></tr></tbody></table></div></div></div></div></div>	Field	Expression	Sample Value	Key	Value	1. Action	act		CEF.DeviceProduct	CPU 410-5H	AppID	CEF.EventName	SE_SESSION_ESTABLISHED	CEF.DeviceVendor	Siemens AG	Bytes_Received	CEF.DeviceVersion	P30.7.0	CEF.DeviceVersion	P30.7.0	Bytes_Sent	in		CEF.EventName	SE_SESSION_ESTABLISHED	CSN_IP	out		CEF.Severity	6	Destination GUID	src	172.16.20.51	CEF.SignatureID	95	Destination IP	dst	172.16.20.100	connType	0x00000106	Destination Mac Address	dmac		dpt	514	Destination Port	dpt	514	dst	172.16.20.100	Destination_Hostname	dhost		dvc	172.16.20.51	Destination_UserID	duid		opmod	RUN	Event Count	cnt		protlevel	3	Filename	fname		proto	TCPnative	First Time	start	MAY 12 2017 14:57:47.262	pid	0	HostID	CEF.DeviceProduct	CPU 410-5H	smac	20:07:56:28:43:dd	Last Time	start	MAY 12 2017 14:57:47.262	spt	49252	Message_Text	CEF.DeviceVendor	Siemens AG	src	172.16.20.51	ObjectID	feature		start	MAY 12 2017 14:57:47.262
Field	Expression	Sample Value	Key	Value																																																																																												
1. Action	act		CEF.DeviceProduct	CPU 410-5H																																																																																												
AppID	CEF.EventName	SE_SESSION_ESTABLISHED	CEF.DeviceVendor	Siemens AG																																																																																												
Bytes_Received	CEF.DeviceVersion	P30.7.0	CEF.DeviceVersion	P30.7.0																																																																																												
Bytes_Sent	in		CEF.EventName	SE_SESSION_ESTABLISHED																																																																																												
CSN_IP	out		CEF.Severity	6																																																																																												
Destination GUID	src	172.16.20.51	CEF.SignatureID	95																																																																																												
Destination IP	dst	172.16.20.100	connType	0x00000106																																																																																												
Destination Mac Address	dmac		dpt	514																																																																																												
Destination Port	dpt	514	dst	172.16.20.100																																																																																												
Destination_Hostname	dhost		dvc	172.16.20.51																																																																																												
Destination_UserID	duid		opmod	RUN																																																																																												
Event Count	cnt		protlevel	3																																																																																												
Filename	fname		proto	TCPnative																																																																																												
First Time	start	MAY 12 2017 14:57:47.262	pid	0																																																																																												
HostID	CEF.DeviceProduct	CPU 410-5H	smac	20:07:56:28:43:dd																																																																																												
Last Time	start	MAY 12 2017 14:57:47.262	spt	49252																																																																																												
Message_Text	CEF.DeviceVendor	Siemens AG	src	172.16.20.51																																																																																												
ObjectID	feature		start	MAY 12 2017 14:57:47.262																																																																																												
10	<div><div>Switch to the "Mapping" tab and check whether the "Action Value" "success" and "failure" are assigned the corresponding events SE_NETWORK_SUCCESSFUL_LOGON or SE_NETWORK_UNSUCCESSFUL_LOGON. Complete this if needed.</div><div><div><div>File Tools Help</div><div>General Parsing Field Assignment Mapping</div><div>Fill out the desired custom fields below. Custom fields are used in rare cases that you might have with particular way that is beyond the norm.</div><div><table><thead><tr><th>Time Format</th><th>Time Fields</th></tr></thead><tbody><tr><td>%Y-%m-%dT%T%.3f</td><td>First Time, Last Time</td></tr></tbody></table></div><div>Match the desired action fields on the left to the different kinds of actions that could occur based off of incoming log data to the right by entering values into the action mapping column.</div><div><table><thead><tr><th>Action Key</th><th>Action Value</th></tr></thead><tbody><tr><td></td><td>error</td></tr><tr><td>SE_NETWORK_SUCCESSFUL_LOGON</td><td>success</td></tr><tr><td>SE_NETWORK_UNSUCCESSFUL_LOGON</td><td>failure</td></tr><tr><td></td><td>emergency</td></tr></tbody></table></div><div><div><input type="checkbox"/> Use the following action for the default if one is not specified</div><div>pass</div></div><div>Severity Mapping:</div><div><table><thead><tr><th>Severity Key</th><th>Severity Value</th></tr></thead><tbody></tbody></table></div></div></div></div>	Time Format	Time Fields	%Y-%m-%dT%T%.3f	First Time, Last Time	Action Key	Action Value		error	SE_NETWORK_SUCCESSFUL_LOGON	success	SE_NETWORK_UNSUCCESSFUL_LOGON	failure		emergency	Severity Key	Severity Value																																																																															
Time Format	Time Fields																																																																																															
%Y-%m-%dT%T%.3f	First Time, Last Time																																																																																															
Action Key	Action Value																																																																																															
	error																																																																																															
SE_NETWORK_SUCCESSFUL_LOGON	success																																																																																															
SE_NETWORK_UNSUCCESSFUL_LOGON	failure																																																																																															
	emergency																																																																																															
Severity Key	Severity Value																																																																																															
11	<div><div>Save the rule using the "Finish" button.</div><div><div><div>Back</div><div>Next ></div><div>Finish</div></div></div></div>																																																																																															
12	<div><div>Start the rollout procedure with the corresponding button.</div></div>																																																																																															

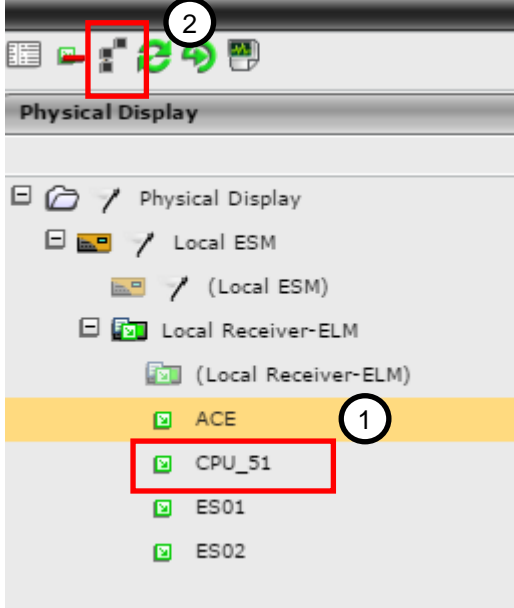
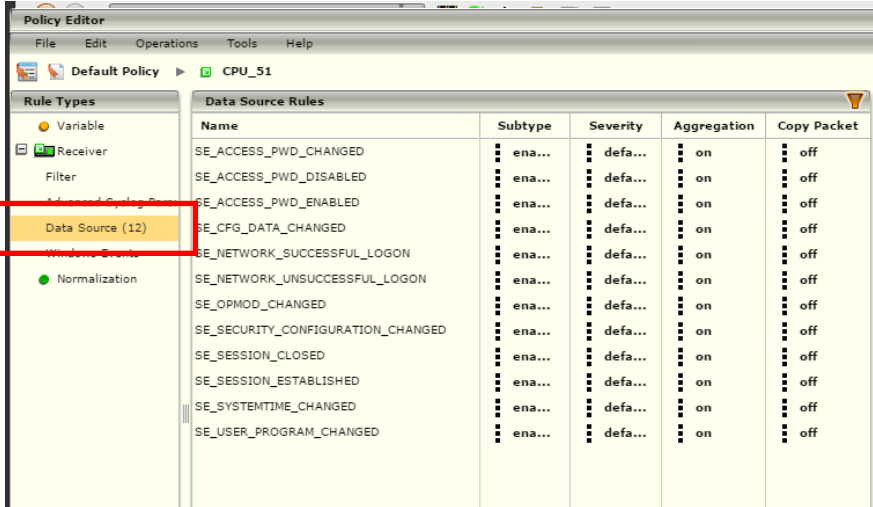
No.	Action
	
13	<p>Confirm the rollout with the "OK" button. Ensure that the option "Rollout policy to all devices now" is enabled.</p>  <p>Note: The name of the displayed components may vary in your configuration.</p>
14	<p>If you want to proceed directly to the next step of the normalization check, you can go to step 4 of the Table 3-3.</p>

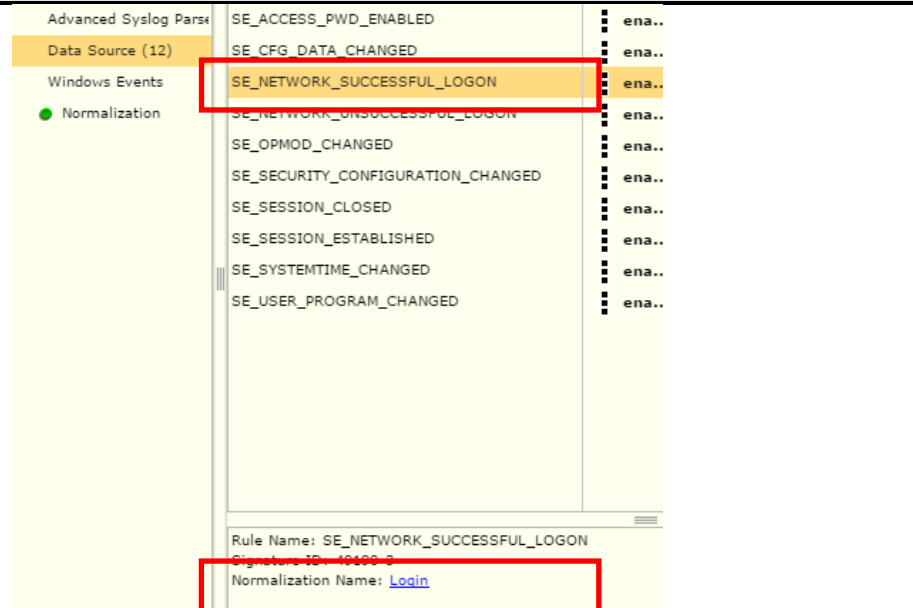
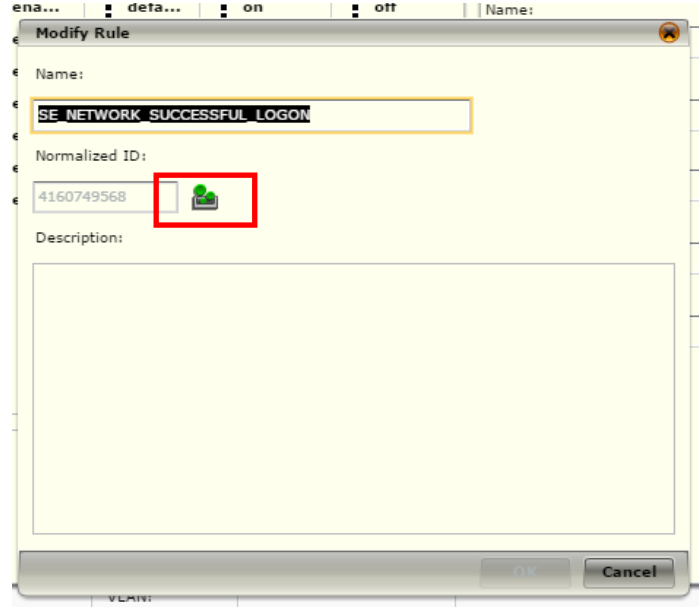
Check the normalization rule of the CPU events

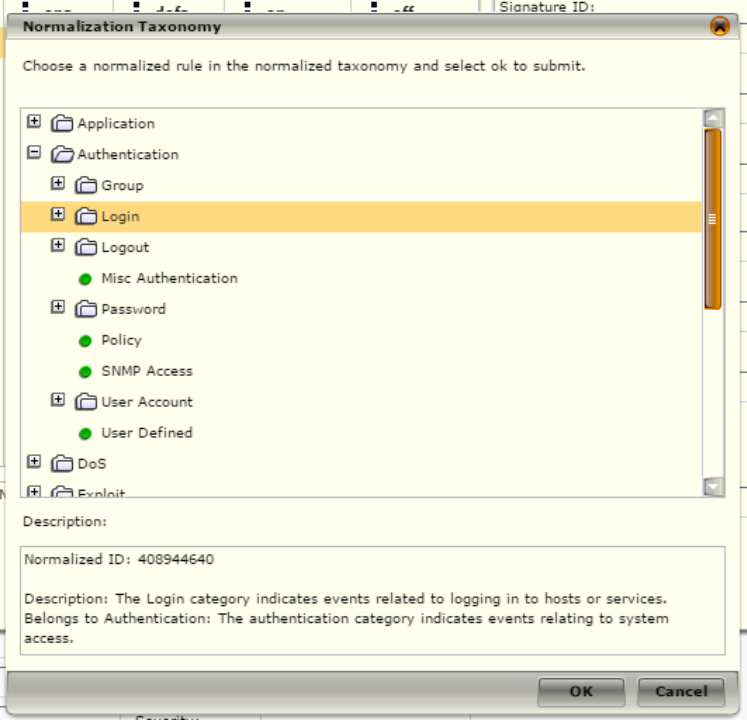
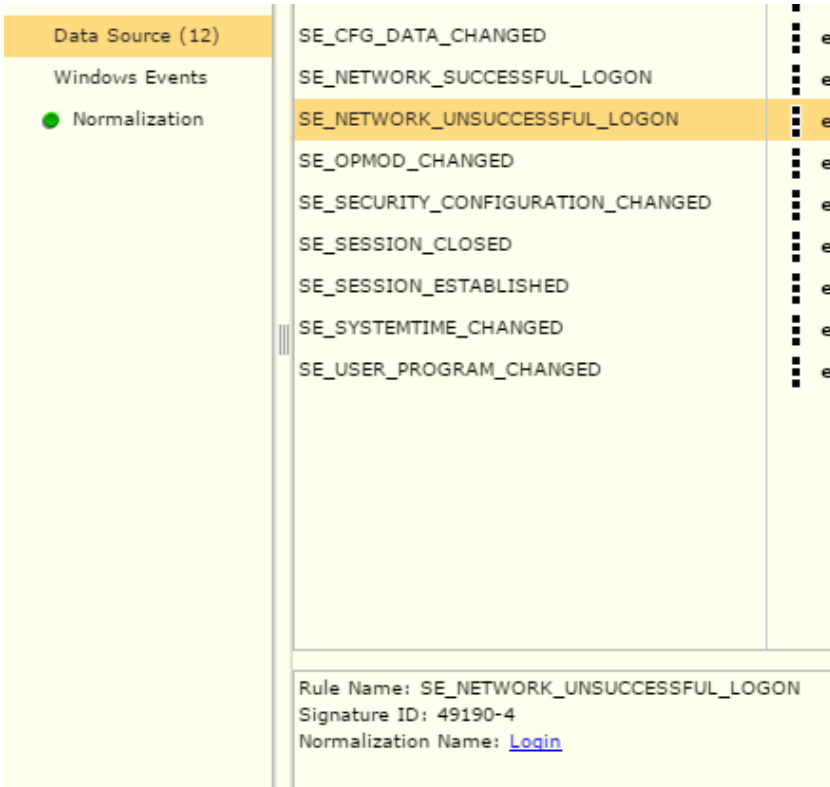
Note To do this, the corresponding events must have been sent to the SIEM system and imported by a SIMATIC controller beforehand.

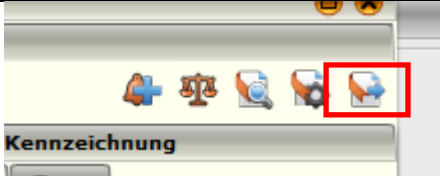
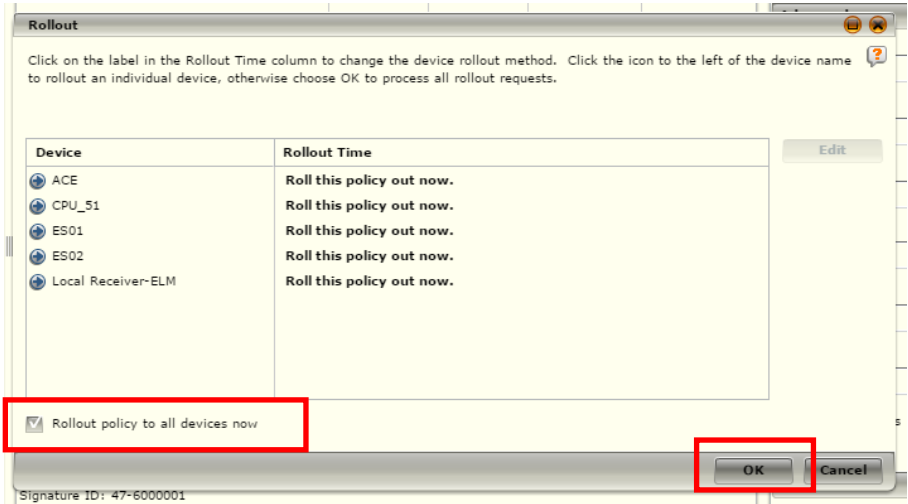
Table 3-3

No.	Action
1.	Open the web-based user interface for McAfee ESM.
2.	Log in with your user name and the password.
3.	Open the Policy Editor (2) of the SIMATIC Controller ("CPU_51" in this case) (1).

No.	Action																																																																	
																																																																		
4.	<p>Select the menu command "Data Source".</p>  <table><thead><tr><th>Name</th><th>Subtype</th><th>Severity</th><th>Aggregation</th><th>Copy Packet</th></tr></thead><tbody><tr><td>SE_ACCESS_PWD_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_ACCESS_PWD_DISABLED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_ACCESS_PWD_ENABLED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_CFG_DATA_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_NETWORK_SUCCESSFUL_LOGON</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_NETWORK_UNSUCCESSFUL_LOGON</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_OPMOD_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_SECURITY_CONFIGURATION_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_SESSION_CLOSED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_SESSION_ESTABLISHED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_SYSTEMTIME_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr><tr><td>SE_USER_PROGRAM_CHANGED</td><td>ena...</td><td>defa...</td><td>on</td><td>off</td></tr></tbody></table>	Name	Subtype	Severity	Aggregation	Copy Packet	SE_ACCESS_PWD_CHANGED	ena...	defa...	on	off	SE_ACCESS_PWD_DISABLED	ena...	defa...	on	off	SE_ACCESS_PWD_ENABLED	ena...	defa...	on	off	SE_CFG_DATA_CHANGED	ena...	defa...	on	off	SE_NETWORK_SUCCESSFUL_LOGON	ena...	defa...	on	off	SE_NETWORK_UNSUCCESSFUL_LOGON	ena...	defa...	on	off	SE_OPMOD_CHANGED	ena...	defa...	on	off	SE_SECURITY_CONFIGURATION_CHANGED	ena...	defa...	on	off	SE_SESSION_CLOSED	ena...	defa...	on	off	SE_SESSION_ESTABLISHED	ena...	defa...	on	off	SE_SYSTEMTIME_CHANGED	ena...	defa...	on	off	SE_USER_PROGRAM_CHANGED	ena...	defa...	on	off
Name	Subtype	Severity	Aggregation	Copy Packet																																																														
SE_ACCESS_PWD_CHANGED	ena...	defa...	on	off																																																														
SE_ACCESS_PWD_DISABLED	ena...	defa...	on	off																																																														
SE_ACCESS_PWD_ENABLED	ena...	defa...	on	off																																																														
SE_CFG_DATA_CHANGED	ena...	defa...	on	off																																																														
SE_NETWORK_SUCCESSFUL_LOGON	ena...	defa...	on	off																																																														
SE_NETWORK_UNSUCCESSFUL_LOGON	ena...	defa...	on	off																																																														
SE_OPMOD_CHANGED	ena...	defa...	on	off																																																														
SE_SECURITY_CONFIGURATION_CHANGED	ena...	defa...	on	off																																																														
SE_SESSION_CLOSED	ena...	defa...	on	off																																																														
SE_SESSION_ESTABLISHED	ena...	defa...	on	off																																																														
SE_SYSTEMTIME_CHANGED	ena...	defa...	on	off																																																														
SE_USER_PROGRAM_CHANGED	ena...	defa...	on	off																																																														
5.	<p>Select the event SE_NETWORK_SUCCESSFUL_LOGON and check whether it is assigned Normalization Name: "Login".</p>																																																																	

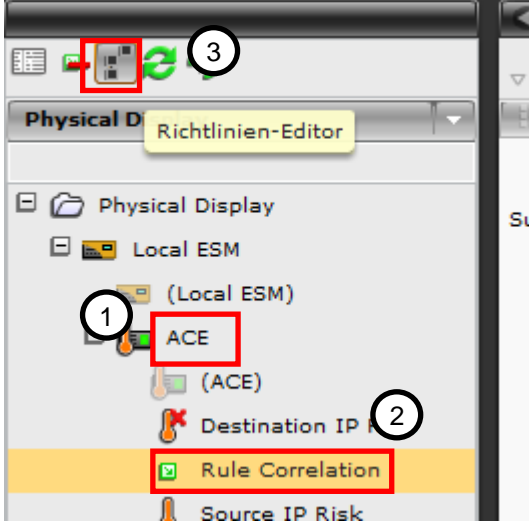
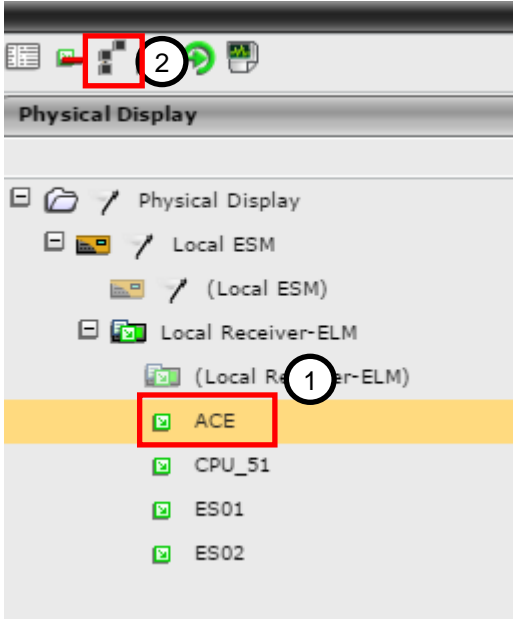
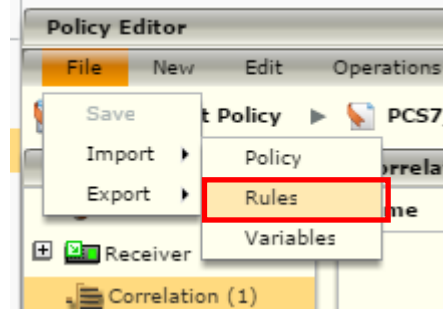
No.	Action
	
6.	<p>If this is not the case, open the properties by double-clicking on the event. Then click on the selection icon.</p> 
7.	<p>In the new window, select the "Login" group, which is assigned to the "Authentication" group.</p>

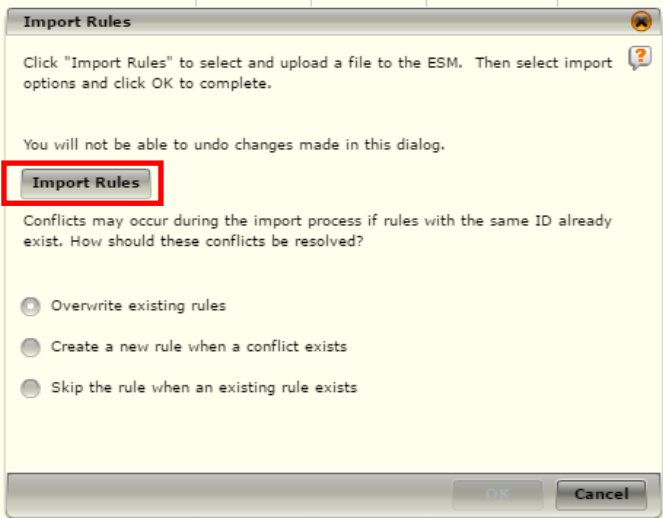
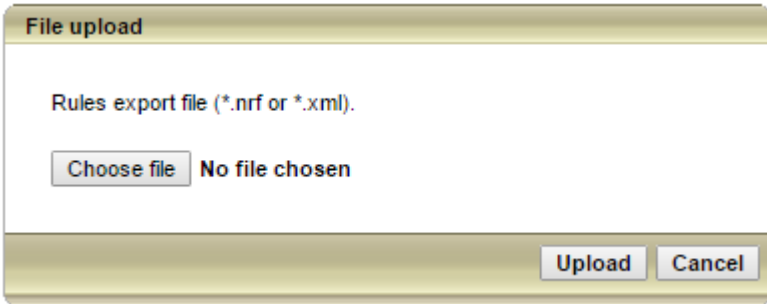
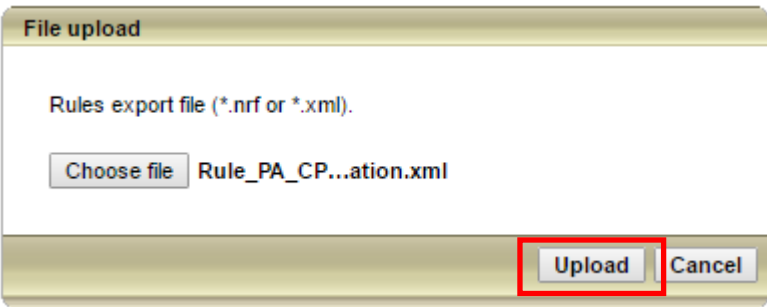
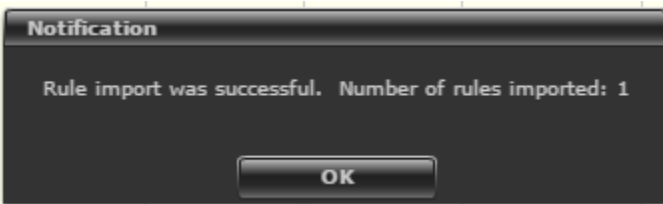
No.	Action
	
8.	Confirm your selection with the "OK" button.
9.	Also close the Properties window by clicking "OK".
10.	<p>Repeat steps 5-9 for the event: SE_NETWORK_UNSUCCESSFUL_LOGON</p> 
11.	Start the rollout procedure with the corresponding button.

No.	Action
	
12.	<p>Confirm the rollout with the "OK" button. Ensure that the option "Rollout policy to all devices now" is enabled.</p>  <p>Note: The name of the displayed components may vary in your configuration.</p>

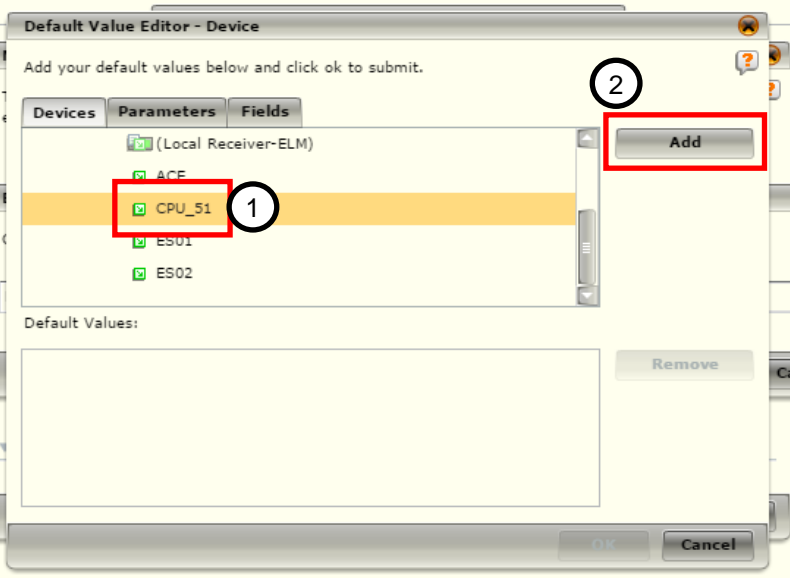

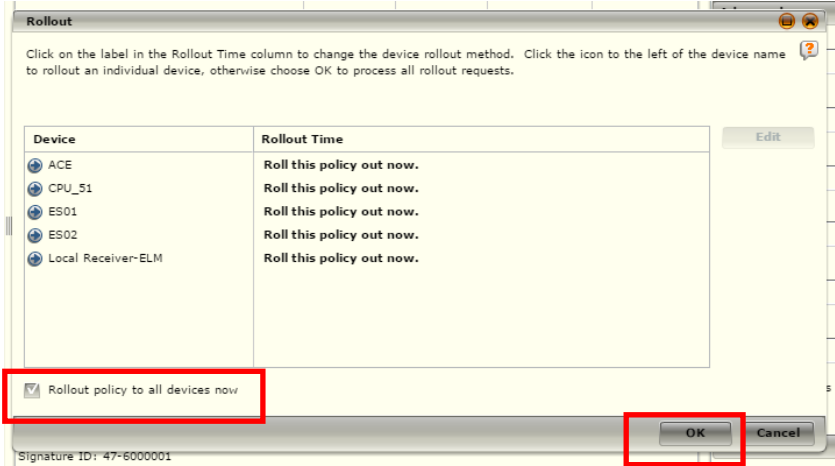
Import the correlation rule for determining the user name

No.	Action
1	Open the web-based user interface for McAfee ESM.
2	Log in with your user name and the password.
3	<p>Select the "Rule Correlation" (2) under "ACE" (1) and open the "Policy Editor" by clicking on the corresponding icon (3).</p> <p>Note: The names of the displayed components may vary with your configuration. In this example, a dedicated "ACE" is used.</p>

No.	Action
	 <p>If the receiver of your system has a correlation engine, your structure might look like this:</p> 
4	<p>In the "File" menu, click "Import > "Rules".</p> 
5	<p>Click on the "Import Rules" button</p>

No.	Action												
	 <p>The "Import Rules" dialog box is shown. It contains instructions to click "Import Rules" to select and upload a file to the ESM. Then select import options and click OK to complete. A red box highlights the "Import Rules" button. Below the instructions, it states: "You will not be able to undo changes made in this dialog." Conflicts may occur during the import process if rules with the same ID already exist. How should these conflicts be resolved?</p> <ul style="list-style-type: none"><input checked="" type="radio"/> Overwrite existing rules<input type="radio"/> Create a new rule when a conflict exists<input type="radio"/> Skip the rule when an existing rule exists <p>At the bottom right are "OK" and "Cancel" buttons.</p>												
6	<p>In the window displayed, click on the "Choose file" button and select the rule provided in your file system.</p>  <p>The "File upload" dialog box is shown. It contains the text "Rules export file (*.nrf or *.xml)." Below this is a "Choose file" button and the text "No file chosen". At the bottom right are "Upload" and "Cancel" buttons.</p>												
7	<p>Start the upload process with the "Upload" button</p>  <p>The "File upload" dialog box is shown. It contains the text "Rules export file (*.nrf or *.xml)." Below this is a "Choose file" button and the text "Rule_PA_CP...ation.xml". At the bottom right, the "Upload" button is highlighted with a red box, next to the "Cancel" button.</p>												
8	<p>Successful rule import is confirmed by the following dialog. Exit the dialog by clicking the OK button.</p>  <p>The "Notification" dialog box is shown. It contains the text "Rule import was successful. Number of rules imported: 1". At the bottom center is an "OK" button.</p>												
9	<p>Call up the settings of the imported rule "CPU User Login" by double-clicking on it.</p> <table><tr><td>ES_Login</td><td>akti...</td><td>50</td><td>an</td></tr><tr><td>PA_CPU_Allowed_User_Login Device ID</td><td>akti...</td><td>50</td><td>aus</td></tr><tr><td>PA_CPU_Allowed_User_Login White List</td><td>akti...</td><td>50</td><td>aus</td></tr></table>	ES_Login	akti...	50	an	PA_CPU_Allowed_User_Login Device ID	akti...	50	aus	PA_CPU_Allowed_User_Login White List	akti...	50	aus
ES_Login	akti...	50	an										
PA_CPU_Allowed_User_Login Device ID	akti...	50	aus										
PA_CPU_Allowed_User_Login White List	akti...	50	aus										


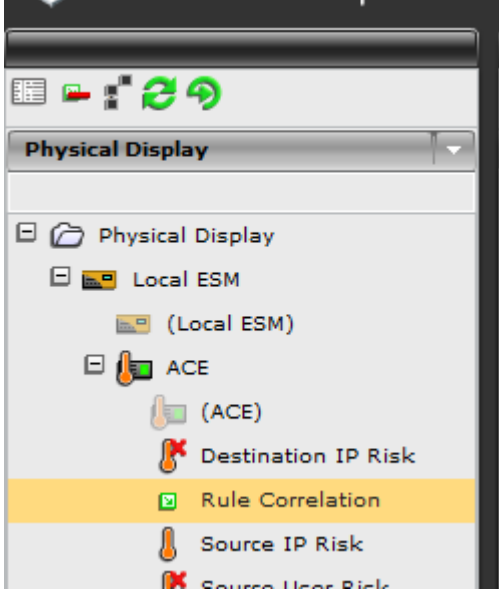

Recording user activity on a SIMATIC Controller
Entry ID: 109748211, V1.0, 06/2017

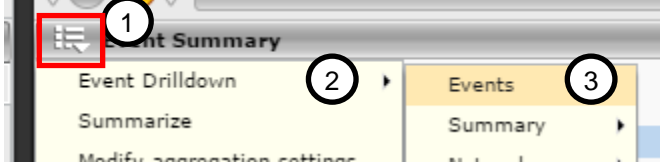
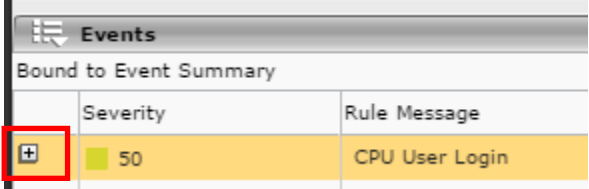
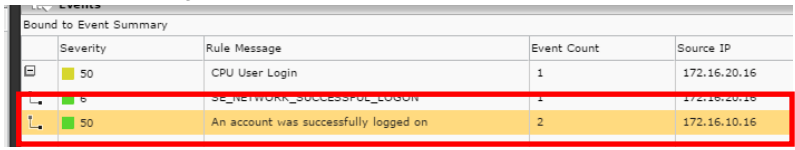
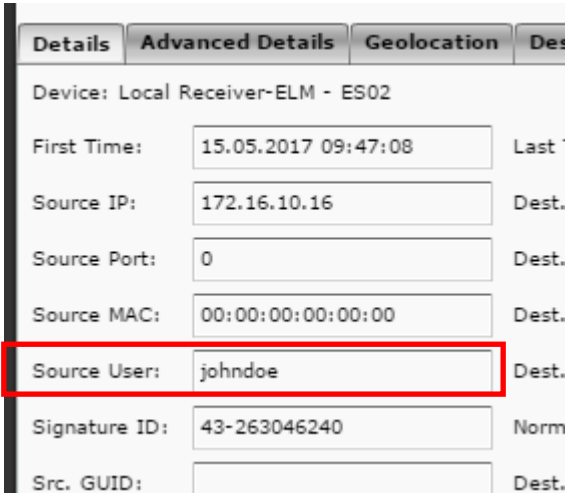
No.	Action
	<p>changes.</p> 
16	Click the "OK" button to save the new filter options of the "Match component" window.
17	Ensure that the rule is enabled in the "Action" column.
18	<p>Roll out the new correlation rule.</p> 
19	<p>Confirm the rollout of the changed rule with the "OK" button. Ensure that the option "Rollout policy to all devices now" is enabled.</p>  <p>Note: The name of the displayed components may vary in your configuration.</p>

4 Function test

[Chapter 3](#) describes the settings to be made for the affected ES and SIMATIC controllers.

To test if all settings have been successfully made and the user name is working, proceed as follows:

No.	Action
1	Log in to an ES with your user name and valid password.
2	Open your PCS 7 project with the SIMATIC controller in SIMATIC Manager. 
3	Make a change on the SIMATIC controller.
4	Download the configuration to the SIMATIC controller.
5	Open the web-based user interface for McAfee ESM.
6	Log in with your user name and the password.
7	Select "ACE" or "Rule Correlation" in the system tree. 
8	In the "Event Summary", the correlation event "CPU User Login" must now be listed.  Note: Depending on the configured update speed, a few minutes may elapse before the correlation result appears.
9	Select the correlation event and open the "Event Drilldown" (2) for "Events" (3).

No.	Action
	
10	<p>Click on the "+" symbol in front of the event listed.</p> 
11	<p>Select the coming event from the ES.</p> 
12	<p>In the "Details" tab, you can find the "Source User", which user has accessed the SIMATIC controller.</p> 

5 List of abbreviations

The following abbreviations are used in this document:

Abbreviation	Definition
ACE	McAfee Advanced Correlation Engine
CSN	Control and System Network
ELM	McAfee Enterprise Log Manager
ERC	McAfee Event Receiver
ES	Engineering Station
ESM	McAfee Enterprise Security Manager
PCN	Process and Control Network
SIEM	Security Information and Event Management
WMI	Windows Management Instrumentation

6 Related literature

	Topic area	Title
\1\	Siemens Industry Online Support	https://support.industry.siemens.com/cs/ww/en/
\2\	Download page for this entry	https://support.industry.siemens.com/cs/ww/en/view/109748211
\3\	Industrial security	https://www.siemens.com/Industrial-Security
\4\	Description of the security events of the SIMATIC controller	http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/tech-doc-pcs7/Pages/Default.aspx
\5\	Security for industrial process measurement and control - Network and system security	https://webstore.iec.ch/publication/7561&preview=1
\6\	Law for increasing the security of information technology systems (IT security law)	http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf (No. 31 from 24/07/2015)
\7\	Data Source Configuration Guide for Microsoft Windows Event Log WMI PD25083	https://kc.mcafee.com/corporate/index?page=content&id=PD25083
\8\	Audit Policy Settings Under Local Policies for Windows Server	https://technet.microsoft.com/en-us/library/dd941595.aspx
\9\	Configuring the Event Logs	https://technet.microsoft.com/en-us/library/dd277416.aspx
\10\	Windows Server - Event Log	https://technet.microsoft.com/en-us/library/dd349798.aspx
\11\	Event Log Policy Settings	https://technet.microsoft.com/en-us/library/cc778402.aspx

7 History

Version	Date	Change
V1.0	06/2017	First version