MaxPatrol SIEM

Expertise Pack. Attacks on Microsoft Active Directory Pack version 3.2

Last edited: 6/29/2023

Contents

1. About this document

This guide contains information about installation of the expertise pack, instructions on how to configure a source for registration of events that are required for the pack to function, and instructions on how to configure MaxPatrol SIEM to collect these events. The guide also describes the information security events registered by MaxPatrol SIEM according to the correlation rules included in the pack.

The guide contains no instructions on how to install, set up, administer MaxPatrol SIEM, or use its main features.

The guide is intended for specialists carrying out MaxPatrol SIEM installation and integration at the organization, and the staff responsible for information security, monitoring, and investigation of incidents.

The MaxPatrol SIEM documentation includes:

- Implementation Guide. How to implement the product on organization infrastructure: standard deployment schemes and instructions on how to install, set up, update, and uninstall the product.
- Administrator Guide. Reference information and instructions for installation, configuration, and administration of the product.
- Security Officer Guide. Scenarios for managing the organization's information assets and information security events.
- Setting Up Sources. Recommendations how to integrate IT infrastructure elements of an enterprise with MaxPatrol SIEM to collect data from sources and audit assets.
- PDQL Syntax. Reference information and examples of syntax, basic features, and operators of the PDQL language that are needed to use MaxPatrol SIEM.
- PDQL Queries for Asset Analysis. Information about standard PDQL queries that are used to check asset configurations in MaxPatrol SIEM.
- Developer Guide. Recommendations on how to create event normalization, enrichment, aggregation, and correlation rules; a description of the MaxPatrol SIEM SDK utilities for debugging; information about the REST API features available in MaxPatrol SIEM.

In this section

1.1. Document conventions

This guide uses the following document conventions.

Table 1. Document conventions

Example	Description
Warning. Disabling the module decreases the level of network security	Warnings. Contain information about actions or events with potentially negative consequences
Note. You can create additional reports	Notes. Contain tips, descriptions of important special cases, and additional or reference information that might be useful
► To open the file:	The beginning of instructions is marked with a specific symbol
Click **OK**	Names of interface elements (for example, buttons, text boxes, and menu items) are highlighted in bold
Run the `Stop-Service` command	Command-line text and code examples that need to be entered using the keyboard are highlighted in a special font. File names and paths to files and folders are also indicated in a special font
CTRL+ALT+DELETE	Key combination. To activate the combination, the keys need to be pressed at the same time
<Application name>	Variables are enclosed in angle brackets

1.2. Other sources of information about MaxPatrol SIEM

You can find additional information about MaxPatrol SIEM on the Technical Support portal.

The portal contains knowledge base articles, news about Positive Technologies product updates, and answers to FAQs. Create a user account on the portal to have access to the knowledge base and all news.

If you cannot find the information you require, please contact Technical Support (see Section 6).

2. About the expertise pack

The pack includes MaxPatrol SIEM correlation rules for registration of information security events related to suspicious activity in a Microsoft Active Directory network. Detected events may indicate ongoing attacks on the organization's IT infrastructure.

The expertise pack is installed automatically when Knowledge Base is updated according to the Implementation Guide.

After the installation and setup of the expertise pack, you must deploy the Knowledge Base database objects to MaxPatrol SIEM.

Table 2. Registered information security events[1]

Information security event	Tactic	Technique
Abuse_Kerberos_RC4. Possible exploitation of the CVE-2022-33679 vulnerability in Kerberos is detected. An attacker attempted to recover the session key of a user to retrieve the authenticated session on their behalf	Credential Access	Steal or Forge Kerberos Tickets
Active_Directory_Snapshot. Creation of an Active Directory structure snapshot using AdExplorer.exe is detected	Discovery	Permission Groups Discovery: Domain Groups
ActiveDirectory_Data_Collection. Execution of an LDAP query to collect domain information using the AD Explorer or SharpHound utility is detected	Discovery	Domain Trust Discovery, Account Discovery: Domain Account, Permission Groups Discovery: Domain Groups, Remote System Discovery
ADCS_Recon. Execution of an LDAP query to search for certification servers in a network is detected	Discovery	Network Service Discovery
AdminSDHolder_Modification_Attack. A new value added to the properties of the AdminSDHolder container is detected. An attacker can gain persistence in the system or obtain elevated privileges	Persistence	Account Manipulation

1 The attack tactics and techniques are given according to the MITRE ATT&CK classification.

Information security event	Tactic	Technique
CA_Cert_Export. Export of the CA certificate that can be used to issue a certificate of any user without knowledge of the password is detected	Credential Access	Steal or Forge Authentication Certificates
Cert_Allowed_Alt_SAN. A request for the certificate that allows the specifying of an alternative SubjectAccountName is detected	Lateral Movement	Use Alternate Authentication Material
Certified_Priv_Esc_CVE_2022_26923. Privilege elevation using the CVE-2022-26923 vulnerability is detected. An attacker modified the DNSHostName attribute value of the domain host and requested a certificate from the certificate authority	Privilege Escalation	Exploitation for Privilege Escalation
Computer_Delegation_Configured. Modification of delegation settings in a domain is detected	Persistence	Modify Authentication Process: Domain Controller Authentication
Copy_Mimikatz_To_Share. Copying of the Mimikatz utility to a shared folder on a remote host is detected. An attacker can operate the utility remotely	Lateral Movement	Lateral Tool Transfer
DACL_Resolver_Aced. Dumping of a discretionary access control list (DACL) for Active Directory objects using the Aced utility is detected	Discovery	Permission Groups Discovery: Domain Groups
DC_Auth_with_Pfx. A TGT request using a certificate or smart card is detected	Lateral Movement	Use Alternate Authentication Material
DCShadow_Attack. A DCShadow attack is detected. An attacker can obtain the credentials of domain users	Defense Evasion	Rogue Domain Controller
DCSync_Attack. A DCSync attack is detected. An attacker can obtain the credentials of domain users	Credential Access	DCsync
DCSync_Privileges_Given. Granting of privileges required for a successful DCSync attack is detected. An attacker can obtain the credentials of domain users	Credential Access	DCsync
DNS_Zone_Transfer_To_Untrusted_Host. A TCP AXFR request from a DNS server not included in the Trusted_DNS_servers tabular list is de-	Discovery	Domain Trust Discovery

Information security event	Tactic	Technique
tected. An attacker can learn more about the structure of the target network using a DNS zone dump		
Enable_SAN_Flag_CA_Policy. Setting of the EDITF_ATTRIBUTESUBJECTALTNAME2 flag that allows the specifying of an alternative SubjectAccountName for all issued certificates is detected	Persistence	Modify Authentication Process: Domain Controller Authentication
gMSA_Password_Access. An attacker accessed the LDAP attributes that store data for generation of group Managed Service Account (gMSA) passwords	Credential Access	Credentials from Password Stores
Golden_Cert. A TGT ticket request using a previously compromised CA certificate is detected. An attacker can use the obtained tickets to recover user password hashes	Credential Access	Steal or Forge Authentication Certificates
Groups_And_Users_Enumeration. Dumping of a list of domain (local) users or groups is detected. An attacker obtained a list of domain users and/or groups	Discovery	Account Discovery
Kerberoasting. A request for TGS tickets with specific encryption types is detected	Credential Access	Steal or Forge Kerberos Tickets: Kerberoasting
Kerberos_Silver_Ticket. A Silver Ticket attack is detected. An attacker issued a forged TGS ticket for an account to access one of the hosts	Credential Access	Steal or Forge Kerberos Tickets: Silver Ticket
KrbRelay_Usage. Signs of using the KrbRelay utility in any way are detected. An attacker created the IMarshal interface on one of the ports or authenticated locally using a Kerberos relayed ticket account	Privilege Escalation, Defense Evasion	Exploitation for Privilege Escalation, Abuse Elevation Control Mechanism: Bypass User Account Control
Potential_domain_groups_and_users_enumeration_handle. An attempt to dump a list of users or groups from the domain controller (a request for the SAM_DOMAIN object handle) is detected. An attacker can obtain a list of domain users and/or groups	Discovery	Account Discovery

Information security event	Tactic	Technique
Potential_localgroups_and_administrators_enumeration_handle. An attempt to dump a list of local admin group users or a list of groups is detected. An attacker can obtain a list of domain users and/or groups	Discovery	Account Discovery
Potential_session_enumeration_process. Startup of a utility for dumping a list of active user sessions is detected. An attacker can obtain the credentials of privileged users	Discovery	Account Discovery
Potential_Users_Or_Groups_Enumeration_Process. An attempt to dump a list of users or groups from the domain controller using the net.exe (net1.exe) process is detected. An attacker can obtain a list of domain users and/or groups	Discovery	Account Discovery
PowerViewPy_RBCD_Attack. Resource-based constrained delegation is detected as set for a domain	Persistence	Account Manipulation
Remote_Actions_With_Domain_Objects. Use of scripts from the PowerView tool is detected	Persistence	Account Manipulation
Replication_to_unauthorized_DRA. Replication of Active Directory with a source not included in the Directory_Replication_Agent tabular list is detected. By creating a fake domain controller, an attacker can modify objects in Active Directory	Discovery	Account Discovery
Session_enumeration_smb. Dumping of a list of active user sessions is detected. An attacker can obtain the credentials of privileged users	Discovery	Account Discovery
SAM_Account_Name_Spoofing. One of the two events is detected: • Changed login of an account (Active Directory object) to one that does not end with the $ character • TGT request on behalf of an account whose login matches the domain controller name but does not end with the $ character	Privilege Escalation	sAMAccountName Spoofing

Information security event	Tactic	Technique
ShadowCred_Used. One of the signs of using the Shadow Credentials technique is detected: • Modification of the msds-keycredentiallink attribute for a directory service object • Using passwordless authentication to get a TGT ticket for a system account	Privilege Escalation, Defense Evasion	Exploitation for Privilege Escalation, Abuse Elevation Control Mechanism: Bypass User Account Control
SIDHistory_Modification_Attack. An sIDHistory attribute added to an account is detected. An attacker can elevate their privileges in the domain	Privilege Escalation	SID-History Injection
Subrule_PowerView_Objects_Actions. Remote change of domain objects (domain users and groups, machine accounts) using the PowerView tool (PowerViewPy) is detected	Persistence	Account Manipulation
Subrule_Tickets_Requested. A request for session tickets to access services is detected	Credential Access	Steal or Forge Kerberos Tickets: Kerberoasting

3. Configuring sources

Servers, workstations, and domain controllers of a Microsoft Active Directory network on Windows Server 2008, 2008 R2, 2012, 2012 R2, or 2016 can be used as event sources for the expertise pack correlation rules. The Microsoft Sysmon service can also serve as a source of events. Events from sources are saved to the Windows event log.

You must configure sources under a user account included in the Administrators group on the domain controller.

> **Warning.** If the corporate IT infrastructure uses a firewall or other means of network traffic control, you must configure rules allowing traffic in both directions between the source host and the MP 10 Agent host. The system TCP port 135 and dynamic TCP ports 49152–65535 are used.
>
> **Warning.** When using Windows Firewall on the source host, you must enable the following inbound rules: Remote Event Log Management (NP-In), Remote Event Log Management (RPC), and Remote Event Log Management (RPC-EPMAP).

To receive Microsoft Sysmon events, you must install the service on workstations, servers, and domain controllers. If the service is installed, you must modify its configuration.

To configure other event sources on the domain controller, you must do the following:

1. Configure logging of LDAP requests in the Windows registry.
2. For servers and workstations, configure command-line process creation auditing in Windows using a group policy.
3. For domain controllers, servers, and workstations, configure the Windows Advanced Audit Policy (AAP) using a group policy.
4. Create and configure a domain account for collecting MP 10 Agent events from the Windows event log by following the instructions in the Setting Up Sources Guide.

   Note. To collect MP 10 Agent events, you can create local operating system user accounts with identical credentials instead of a domain account on all domain controllers, servers, and workstations. You must add each user account to the "Access this computer from the network" local security policy and the Event Log Readers local user group. You must add one user account with credentials shared by all accounts to MaxPatrol SIEM.

In this section

3.1. Selecting event sources

To register an information security event according to the pack correlation rules, you must configure logging of certain events on the sources specified in the table below. Configuration of one available source is sufficient.

For Windows auditing, the table lists Windows security system event IDs (for example, 4688 for the "A new process has been created" event); for Sysmon, the table lists event type IDs specified in the Sysmon configuration file (for example, 1 for the "Process creation" events). Configuration of event logging is described in the corresponding sections below.

Table 3. Event sources and IDs required for registration of information security events

Information security event	Event source	
	Windows advanced audit	Sysmon service
Abuse_Kerberos_RC4	4768, 4769, 4771	—
Active_Directory_Snapshot	1644	—
ActiveDirectory_Data_Collection	1644	—
ADCS_Recon	1644	—
AdminSDHolder_Modification_Attack	5136	—
CA_Cert_Export	4688, 5059, 5145	—
Cert_Allowed_Alt_SAN	4887, 4888, 4898	—
Certified_Priv_Esc_CVE_2022_26923	4741, 5136, 5145	—
Computer_Delegation_Configured	5136	—
Copy_Mimikatz_To_Share	5145	—
DACL_Resolver_Aced	1644	—
DC_Auth_with_Pfx	4768	—
DCShadow_Attack	4624, 4742	—
DCSync_Attack	4624, 4662	—
DCSync_Privileges_Given	5136	—
DNS_Zone_Transfer_To_Untrusted_Host	6001, 6525	—
Enable_SAN_Flag_CA_Policy	—	13
gMSA_Password_Access	4662	—

Information security event	Event source	
	Windows advanced audit	Sysmon service
Golden_Cert	4688, 4768, 5059, 5145	—
Groups_And_Users_Enumeration	4624, 4661	—
Kerberoasting	1644, 4769	—
Kerberos_Silver_Ticket	4624	—
KrbRelay_Usage	4624, 5156	3
Potential_domain_groups_and_users_enumeration_handle	4624, 4661	—
Potential_localgroups_and_administrators_enumeration_handle	4624, 4661	—
Potential_session_enumeration_process	4688	1
Potential_Users_Or_Groups_Enumeration_Process	4688	1
PowerViewPy_RBCD_Attack	1644, 5136	—
Remote_Actions_With_Domain_Objects	1644, 4720, 4724, 4726, 4728, 4729, 4732, 4733, 4738, 4741, 4742, 4743, 5136	—
Replication_to_unauthorized_DRA	4928, 4929	—
SAM_Account_Name_Spoofing	4742, 4768	—
Session_enumeration_smb	4624, 5145	—
ShadowCred_Used	1644, 4768, 5136	—
SIDHistory_Modification_Attack	4738, 5136	—
Subrule_PowerView_Objects_Actions	1644	—
Subrule_Tickets_Requested	—	—

3.2. Configuring LDAP request logging

To register Windows security events with ID 1644, you must configure logging of LDAP requests using the registry editor.

► To configure LDAP request logging:

1. Click **Start** → **Run**.
2. In the **Open** box, enter `regedit`, and click **OK**.

   The **Registry Editor** window opens.
3. In the left pane, select the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Diagnostics` node.
4. Select the **15 Field Engineering** value.

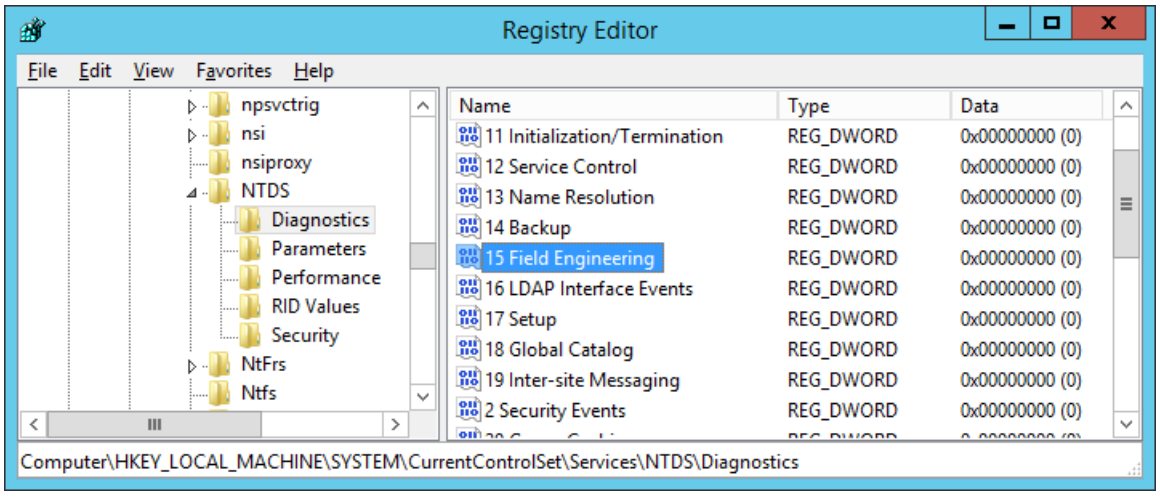

Figure 1. Selecting the 15 Field Engineering value

5. On the main menu, click **Edit** → **Modify**.
6. Under **Base**, select **Decimal**.
7. In the **Value data** box, enter `5`, and click **OK**.

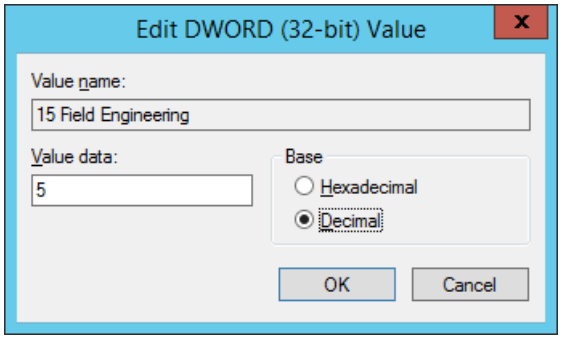

Figure 2. Modifying the 15 Field Engineering value

8. In the left pane, select the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` node.
9. On the main menu, click **Edit** → **New** → **DWORD (32-bit) Value**.

10. Enter the name of the newly created value: `Expensive Search Results Threshold`.
11. On the main menu, click **Edit** → **Modify**.
12. Under **Base**, select **Decimal**.
13. In the **Value data** box, enter `1`, and click **OK**.

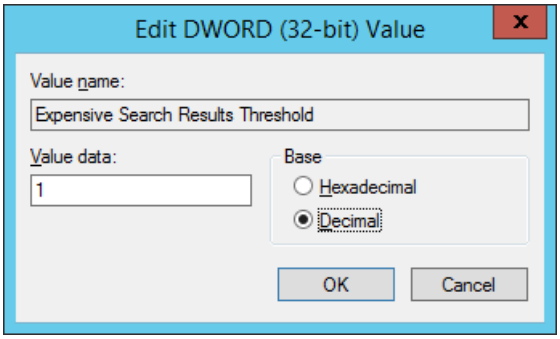

Figure 3. Modifying the Expensive Search Results Threshold value

14. On the main menu, click **Edit** → **New** → **DWORD (32-bit) Value**.
15. Enter the name of the newly created value: `Inefficient Search Results Threshold`.
16. On the main menu, click **Edit** → **Modify**.
17. Under **Base**, select **Decimal**.
18. In the **Value data** box, enter `1`, and click **OK**.

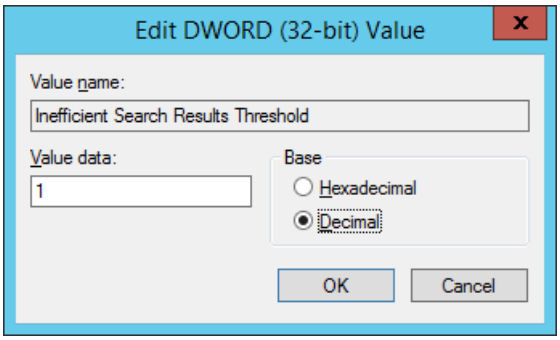

Figure 4. Modifying the Inefficient Search Results Threshold value

LDAP request logging is configured.

3.3. Configuring the Advanced Audit Policy via a group policy

You must configure the Advanced Audit Policy on the asset domain controller via a group policy as shown in the table below.

Table 4. Configuring the Advanced Audit Policy

ID	Category	Subcategory	Audit type
4624	Logon/Logout	Audit Logon	Success
4661	Object Access; Directory Service	Audit Kernel Object, Audit SAM; Audit Directory Service Access	Success
4662	Directory Service	Audit Directory Service Access	Success
4688[2]	Detailed Tracking	Audit Process Creation	Success
4720, 4724, 4726	User Account Management	Audit User Account Management	Success
4728, 4729, 4732, 4733	User Account Management	Audit Security Group Management	Success
4738	User Account Management	Audit User Account Management	Success
4741, 4743	User Account Management	Audit Computer Account Management	Success
4742	User Account Management	Audit Computer Account Management	Success
4768	Account Logon	Audit Kerberos Authentication Service	Success, Failure
4769	Account Logon	Audit Kerberos Service Ticket Operations	Success, Failure
4771	Account Logon	Audit Kerberos Authentication Service	Failure
4887	Object Access	Audit Certification Services	Success
4888	Object Access	Audit Certification Services	Failure

2 To register the event, you must also configure inclusion of the command line in process creation events using a group policy.

ID	Category	Subcategory	Audit type
4898	Object Access	Audit Certification Services	Success
4928	Directory Service	Audit Directory Service Replication	Success
4929	Directory Service	Audit Detailed Directory Service Replication	Success
5059	System	Audit Other System Events	Success
5136	Directory Service	Audit Directory Service Changes	Success
5145	Object Access	Audit Detailed File Share	Success, Failure
5156	Object Access	Audit Filtering Platform Connection	Success

- To configure the Advanced Audit Policy via a group policy:

  1. Open the Windows Control Panel.
  2. Select **Administrative Tools** → **Group Policy Management**.

     The Group Policy Management Console is launched.

     Note. You can also launch the Group Policy Management Console by executing the `gpmc.msc` command.
  3. In the left pane, select the node of the policy being used: **Group Policy Management** → **Forest: <forest name>** → **Domains** → **<Domain name>** → **<Servers or workstations group policy name>**.
  4. On the main menu, click **Action** → **Edit**.

     The **Group Policy Management Editor** window opens.
  5. In the left pane, select the node **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies** → **<Category name>**.
  6. Select an audit policy subcategory.

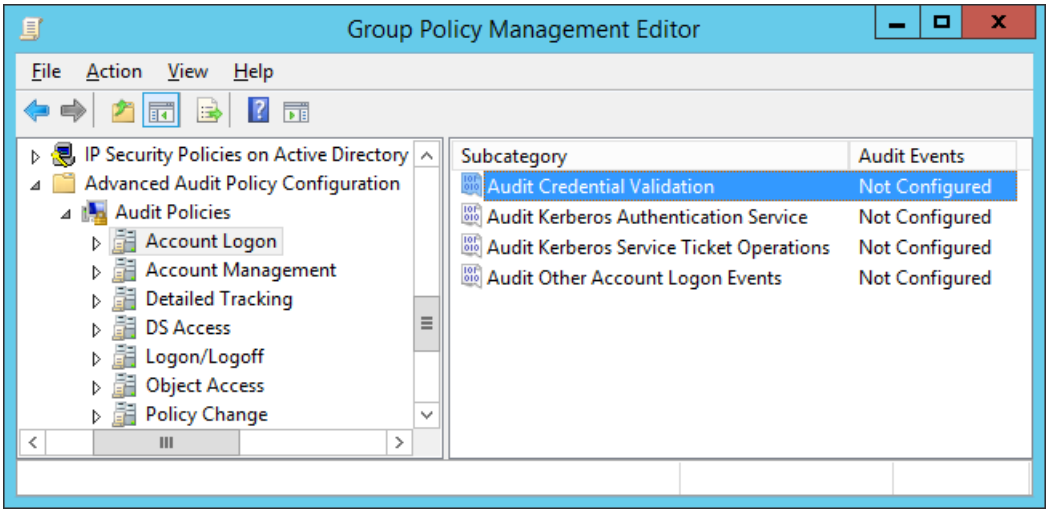

Figure 5. Selecting an audit policy subcategory

7. On the main menu, click **Action** → **Properties**.
8. In the window that opens, select the **Configure the following audit events** check box.
9. To enable success audit, select the **Success** check box.
10. To enable failure audit, select the **Failure** check box.

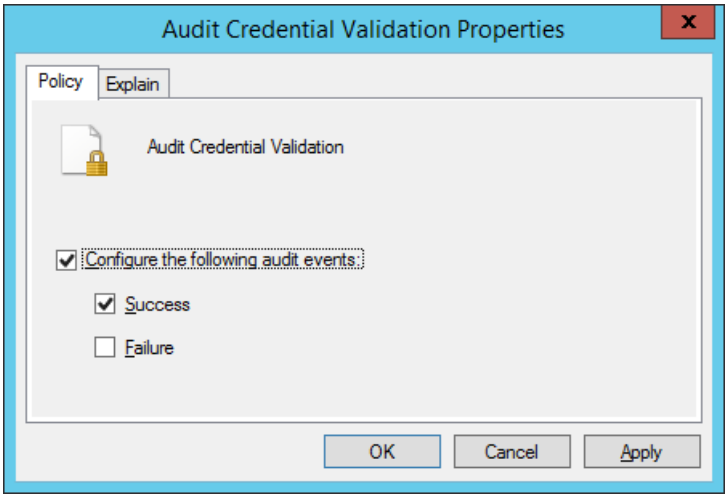

Figure 6. Configuring an audit policy subcategory

11. Click **OK**.

The Advanced Audit Policy is configured.

3.4. Configuring the Microsoft Sysmon service

Note. These instructions are designed for Microsoft Sysmon version 13.34 (with configuration schema version 4.81) or later.

You must install the Microsoft Sysmon service on the asset or, if it is already installed, modify the service settings. The service configuration file is available by clicking the **Sysmon configuration file** link on the pack description page in Knowledge Base. You can also download the archived configuration file from storage.ptsecurity.com.

Installing Microsoft Sysmon

You can download an installer for Microsoft Sysmon from docs.microsoft.com.

- To install Microsoft Sysmon:

  1. Open the Windows command-line interface as an administrator.
  2. Execute the installer:
     ```
     sysmon.exe -i <path to configuration file>
     ```
  3. In the window that opens, click **Agree**.

  The service is installed.

Changing the Microsoft Sysmon configuration

- To change the Microsoft Sysmon configuration:

  1. Add the event filters specified in the downloaded configuration file to the `EventFiltering` section of the Microsoft Sysmon configuration file.
  2. Open the Windows command-line interface as an administrator.
  3. Execute the installer:
     ```
     sysmon.exe -c <path to configuration file>
     ```

  The configuration of the service is changed.

4. Configuring MaxPatrol SIEM

To collect source events from an asset in MaxPatrol SIEM, you must do the following:

1. Add an operating system credential for accessing the asset.
2. Create and start a task for collecting events from the Windows log with the WinEventLogMSAD profile.
3. Create and start a task for collecting Microsoft Sysmon events with the WinEventLogSysmon profile.

In this section

4.1. Adding an operating system credential

► To add a credential for accessing the source to MaxPatrol SIEM:

1. On the main menu, click **Data collection**, and then click **Credentials**.

   The **Credentials** page opens.

2. On the toolbar, click **Add credential**, and on the menu that opens, click **Login–Password**.

   The **Add credential** page opens.

3. In the **Name** box, enter a name for the credential.

   Note. In the **Description** box, enter any text comment.

4. In the **Tags** list, select the **WindowsLogs** check box.
5. In the **Login** box, enter the account login.
6. If required, in the **Password** box, type a password and confirm it in the **Confirm password** box.
7. If using a domain account to access the source, in the **Domain** box, enter a domain name.
8. Click **Save**.

The credential is added.

4.2. Creating and starting an event collection task

- To create and start a task for collecting events from the source:

  1. On the main menu, click **Data collection**, and then click **Tasks**.

     The **Data collection tasks** page opens.

  2. On the toolbar, click **Create task**, and on the menu that opens, click **Data collection**.

     The **Create data collection task** page opens.

  3. In the **Name** box, enter a name for the task.
  4. In the **Profile** list, select **WinEventLogMSAD**.
  5. In the **Credential** list, select a credential for accessing the source.
  6. If required, in the **Agent** list, select an MP 10 Agent for event collection.
  7. In the **Data collection targets** panel, on the **Include** tab, in the **Network addresses** box, enter the IP address of the event source.

     Note. In the **Schedule** panel, you can enable and configure the scheduled task start.

  8. Click **Save and start**.

  The task for collecting events from the source is created and started.

4.3. Creating and starting a task for collecting Microsoft Sysmon events

- To create and start a task for collecting events from the source:

  1. On the main menu, click **Data collection**, and then click **Tasks**.

     The **Data collection tasks** page opens.

  2. On the toolbar, click **Create task**, and on the menu that opens, click **Data collection**.

     The **Create data collection task** page opens.

  3. In the **Name** box, enter a name for the task.
  4. In the **Profile** list, select **WinEventLogSysmon**.
  5. In the **Credential** list, select an OS user credential.
  6. If required, in the **Agent** list, select an MP 10 Agent for event collection.
  7. In the **Data collection targets** panel, on the **Include** tab, in the **Network addresses** box, enter the IP address of the event source.

Note. In the **Schedule** panel, you can enable and configure the scheduled task start.

8. Click **Save and start**.

The task for collecting events from the source is created and started.

5. Incident investigation

Analysis of the information security event related to an incident aids its investigation. From the values of event fields, you can obtain the following information:

- `dst.ip`, `dst.fqdn`, or `dst.host`. The IP address and fully qualified domain name (FQDN) of the host targeted by an attack (`dst.port` is the connection port).
- `event_src.ip`, `event_src.fqdn`, or `event_src.host`. The IP address and fully qualified domain name (FQDN) of the host where the incident was registered.
- `src.ip`, `src.fqdn`, or `src.host`. The IP address and FQDN of the host with which the suspicious activity is associated.
- `subject.account.id`, `subject.account.name`, `subject.account.domain`. The ID, login, and domain name of the account with which the suspicious activity is associated.

  Note. You can obtain additional information about the attacker's actions by analyzing events associated with their user account and the host where the suspicious activity is detected.

Incident response

If the detected activity is unexpected or illegitimate for the account, it is recommended to lock the account or isolate the host where the attack originated.

If a false positive is identified, you must configure resolving of false positives. To do this, you must add data related to the information security event associated with the incident to a tabular list of exclusions.

You can use the Common_whitelist_value and Common_whitelist_regex whitelists and the Common_blacklist_value and Common_blacklist_regex blacklists. Tabular lists whose name ends with "value" can be populated by clicking the information security event summary in the MaxPatrol SIEM interface; tabular lists ending with "regex" can only be populated manually. Exclusions in blacklists have a higher priority than those in whitelists.

If you populate tabular lists manually, you must enter the following values in the columns:

- **rule**. The name of the correlation rule used to register the event (specified in the `correlation_name` event field).

  Note. All columns of the tabular list, except **rule**, must be populated in lowercase. Also, if a column can take any value, you must enter an asterisk (*) in a String column or 0 in a Number column.
- **host**. The name of the host where the event was registered (specified in the `event_src.host` field).
- **user_id**. The ID of the account with which the suspicious activity is associated (specified in the `subject.account.id` field).
- **specific_value**. Additional information about the event (specified in the `alert.key` field).

- **specific_regex**. A regular expression (PCRE) that provides additional information about the event (constructed from the data specified in the `alert.key` field).
- **user_name**. The login of the account with which the suspicious activity is associated (specified in the `subject.account.name` field).

  Note. The values in the **user_name** and **user_domain** columns are entered for reference only and not used for event filtering.
- **user_domain**. The domain name of the account with which the suspicious activity is associated (specified in the `subject.account.domain` field).
- **comments**. Any text comment.
- **exclude**. To disable registration of information security incidents and events, you must enter `yes` in the blacklists.

  Note. Exclusions for which `yes` is entered in the **exclude** column are high-priority ones. You can use this to distinguish specific instances of exclusions from more general exclusions in blacklists.

6. Contacting Technical Support

Technical Support includes the following services:

- Help with queries about product usage and features
- Diagnostics, including pinpointing the causes of failures and informing the client of identified issues
- Resolution of product-related problems, and providing solutions or workarounds that maintain necessary performance
- Correcting product-related bugs (as part of product update releases)

You can obtain Technical Support at the online portal.

This section describes how to get Technical Support and the terms and conditions for using the service.

In this section

6.1. Technical Support online

You can request help on the Technical Support online portal.

You can create a portal account using email addresses on your organization's official domain. You can specify other email addresses as secondary addresses for the account. For quicker response, specify the name of your organization and contact phone number in the account profile.

The portal contains knowledge base articles, news about Positive Technologies product updates, and answers to FAQs. Create a user account on the portal to have access to the knowledge base and all news.

Technical Support online is available in English and Russian.

6.2. Technical Support working hours

You can create and update support requests, read news, and access the knowledge base online 24/7.

6.3. How Technical Support processes requests

When your request is received, Technical Support classifies it by type and severity in order to take further steps.

In this section

6.3.1. Providing information for Technical Support

When requested by a Positive Technologies support specialist, please provide:

- Product license number
- Log files and other diagnostic data stored in the product
- Screenshots
- Results of implementing Technical Support recommendations
- Remote access to the product (the particular access method best for diagnostics is decided by mutual agreement)

Positive Technologies has no obligation to provide Technical Support services if the above information is not provided.

If information needed for the request is not provided within a reasonable period of time (two weeks from the date of the most recent activity), Technical Support may close the request and notify you accordingly.

6.3.2. Request types

Technical Support assigns one of the following types to each request.

Queries regarding installation, reinstallation, and pre-start configuration of the product

Covers product setup and initial use. Technical Support of this type is available for 30 days following activation of the product.

Queries regarding product administration and configuration

Covers questions related to product use and recommendations for product optimization and configuration.

Restoring the product

In the event of a critical failure and/or unavailability of core functionality, a Positive Technologies specialist will assist with restoring the product. Restoration involves either reinstallation of the product (potentially causing loss of data) or rollback to a backup (if backups have been created prior to when the problem occurred). Positive Technologies is not responsible for data loss in case of faulty backups.

Updating the product

Positive Technologies supplies updates for the period specified in the license terms.

Positive Technologies is not responsible for problems caused by failure to follow proper update practices.

If a bug is found

If diagnostic analysis identifies a defect in the product, Positive Technologies shall make reasonable efforts to provide a workaround (if possible) and fix the defect in the earliest possible update.

6.3.3. Response time and request prioritization

Response time is defined as the time from receipt of a support request until Technical Support responds with a notification that work has been started on your request.

Processing time is defined as the time from when work is started on your request until Technical Support describes steps for resolving the problem, or until Technical Support classifies the issue as a software defect and refers it to the relevant development team.

Response time and processing time depend on the severity level (see Table 5) that you indicate in your request.

Technical Support may adjust the severity level of a request based on the criteria listed below. Every reasonable effort will be made to comply with the target deadline, but an extension may be required in exceptional circumstances.

Table 5. Response and processing time

Severity level	Severity criteria	Response time	Processing time
Critical	Emergencies that fully prevent the product from operating normally (not including initial installation) or have a critical impact on business activity	Within 4 hours	No limit

Severity level	Severity criteria	Response time	Processing time
High	Failures partially affecting product functionality and arising in all operating conditions, or having a significant impact on business activity	Within 24 hours	No limit
Normal	Failures arising in specific operating conditions or not having a significant impact on business activity	Within 24 hours	No limit
Low	Questions of an informational nature or failures that do not impact product use	Within 24 hours	No limit

Response time and processing time are defined in terms of Technical Support working hours.

6.3.4. Request processing

As your request is processed, Technical Support will inform you of:

- Diagnostic analysis and results
- Solutions and ways to work around the causes of the problem
- Planning and release of product updates (if required to resolve the problem)

If changes to the product are required to resolve the problem, Positive Technologies shall include a patch in the earliest possible product update (depending on the complexity of changes required).

The request shall be considered closed if:

- A solution or workaround is delivered that does not impact the performance or a critically important function of the product.
- A bug in the product is diagnosed, technical information is collected about the bug and the conditions for reproducing it, and the bug is due to be fixed as part of a subsequent product update.
- The problem is identified as having been caused by third-party software or hardware not covered under the warranty.
- The problem is classified as an unsupported type.

positive technologies

Positive Technologies is an industry leader in results-oriented cybersecurity and a major global provider of information security solutions. For 21 years, our mission has been to safeguard businesses and entire industries against the threat of cyberattacks. Over 3,000 organizations worldwide use technologies and services developed by our company. Positive Technologies is the first and only cybersecurity company in Russia to have gone public on the Moscow Exchange (MOEX: POSI), with 165,000 shareholders and counting.