Which Windows events are used by Splunk UBA?

The raw parser in Splunk UBA doesn't look for specific Windows events, Rather, all Windows events are analyzed to find common field names such as account name or workstation. These field names are extracted from Windows events and stored in data cubes to be consumed by anomaly rules and models. Having the right Windows events in Splunk UBA can lead to meaningful detections so that the desired security use cases are unlocked.

See the following categories of Windows events used by Splunk UBA:

- Highly recommended Windows events used by Splunk UBA
- Recommended Windows events used by Splunk UBA
- Nice to have Windows events used by Splunk UBA

Highly recommended Windows events used by Splunk UBA

Ingest the events listed in this table so that Splunk UBA can generate the proper anomalies and threats. To identify the anomalies and threats generated by Windows events, see Which data sources to I need? .

> ⓘ NOTE: The absence of any of the listed events will prevent anomalies and threats from being generated.

Recommended Windows events used by Splunk UBA

It is recommended to log the following Windows event types so that Splunk UBA can generate anomalies and threats.

Windows Event ID	Description
1102	The audit log was cleared.

Nice to have Windows events used by Splunk UBA

The following Windows event types enhance the fidelity of your detections by providing additional evidence and clarity.

Windows Event ID	Description
Windows PowerShell events	
4103	PowerShell Module Logging. See Configure PowerShell logging to see PowerShell anomalies in Splunk UBA.
4104	PowerShell Script Block Logging. See Configure PowerShell logging to see PowerShell anomalies in Splunk UBA.
4688	A new process has been created.
7045	A service was installed in the system.
Windows object and registry handling events	
4657	A registry value was modified.
4691	Indirect access to an object was requested.
4692	Backup of data protection master key was attempted.
4693	Recovery of data protection master key was attempted.
4695	Unprotection of auditable protected data was attempted.
4907	Auditing settings on object were changed.
4911	Resource attributes of the object were changed.
5145	A network share object was checked to see whether client can be granted desired access.
Windows domain, trust, and authentication events	
4706	A new trust was created to a domain.
4713	Kerberos policy was changed.
4715	The audit policy (SACL) on an object was changed.
4770	A Kerberos service ticket was renewed.
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.
4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
Windows policy events	
6273	Network Policy Server denied access to a user.

6276	Network Policy Server quarantined a user.
6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
Windows account handling events	
4627	Group membership information.
4672	Special privileges assigned to new logon.
4704	A user right was assigned.
4718	System security access was removed from an account.
4719	System audit policy was changed.
4720	A user account was created.
4723	An attempt was made to change an account password.
4724	An attempt was made to reset an account password.
4726	A user account was deleted.
4727	A security-enabled global group was created.
4728	A member was added to a security-enabled global group.
4729	A member was removed from a security-enabled global group.
4730	A security-enabled global group was deleted.
4731	A security-enabled local group was created.
4732	A member was added to a security-enabled local group.
4733	A member was removed from a security-enabled local group.
4734	A security-enabled local group was deleted.
4735	A security-enabled local group was changed.
4737	A security-enabled global group was changed.
4744	A security-disabled local group was created.
4745	A security-disabled local group was changed.
4746	A member was added to a security-disabled local group.
4747	A member was removed from a security-disabled local group.
4750	A security-disabled global group was changed.
4754	A security-enabled universal group was created.

4755	A security-enabled universal group was changed.
4756	A member was added to a security-enabled universal group.
4757	A member was removed from a security-enabled universal group.
4758	A security-enabled universal group was deleted.
4759	A security-disabled universal group was created.
4760	A security-disabled universal group was changed.
4761	A member was added to a security-disabled universal group.
4763	A security-disabled universal group was deleted.
4767	A user account was unlocked.
4781	The name of an account was changed.
4782	The password hash an account was accessed.
4797	An attempt was made to query the existence of a blank password for an account.
4798	A user's local group membership was enumerated.
4799	A security-enabled local group membership was enumerated.
Windows device handling events	
4800	The workstation was locked.
4801	The workstation was unlocked.
6416	A new external device was recognized by the system.
Windows security incidents events	
4618	A monitored security event pattern has occurred.
4649	A replay attack was detected.
Windows firewall policy changes events	
4946	A change has been made to Windows Firewall exception list. A rule was added.
4947	A change has been made to Windows Firewall exception list. A rule was modified.
4948	A change has been made to Windows Firewall exception list. A rule was deleted.
4950	A Windows Firewall setting has changed.

Windows events supported by Lateral movement model

The following table lists the Windows events that the UBA Lateral movement model supports:

Windows Event ID	Description
528	Successful logon
529	Logon Failure Unknown user
530	Logon Failure Account logon time
531	Logon Failure Account currently disabled
532	Logon Failure Account expired
533	User Not allowed to logon at this computer
534	Logon Failure not granted logon type
535	Logon Failure Account pass expired
536	Logon Failure Netlogon not active
537	Logon failed for other reasons
538	User logoff
539	Logon failure, Account lockout
540	Successful Network Logon
551	User initiated logoff
552	Logon attempt user explicit creds
576	Special Privileges assigned to new login
593	A process has been exited
627	Changed password attempt
636	Security Enabled local group member added
642	User Account Changed
644	User Account Locked out
648	Security Disabled Local Group Created
649	Security Disabled Local Group Changed
650	Security disabled member removed
651	Security disabled local group member removed
671	User Account Unlocked
672	Authentication Ticket Granted
673	Service Ticket Granted

674	Ticket Granted Renewed
675	Pre-authentication failed
676	Authentication Ticket Request Failed
680	Account used for logon by
681	The logon to account from workstation failed
682	Session reconnected to winstation
683	Session disconnected from winstation
1102	Audit log was clear
4618	A monitored security event pattern has occurred
4624	An account was successfully logged on
4625	Account failed to logon
4627	Group membership information
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4649	A replay attack was detected
4663	An attempt was made to access an object
4672	Special Privileges assigned to new Logon
4673	A privilege service was called.
4674	An operation was attempted on a privilege object
4688	Process created
4689	Process exit
4692	Backup of data protection master key was attempted
4693	Recovery of data protection master key was attempted
4695	Unprotection of auditable protected data was attempted
4696	A primary token was assigned to process
4698	A scheduled task was created.
4718	System security access was removed from an account
4720	A user account was created

4722	A user account was enabled
4723	An attempt was made to change an account password.
4724	An attempt was made to reset an account password.
4725	A user account was disabled
4726	A user account was deleted
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4732	A member was added to a security enabled local group
4733	A member was removed from a security-enabled local group
4738	A user account was changed
4738	A user account was changed
4740	User account locked
4741	A computer account was created
4742	A computer account was changed
4743	A computer account was deleted
4744	A security disable group was created
4745	A security disable local group was changed
4746	A member was added to a sec-disd local group
4747	A member was removed from sec-dis local group
4756	A member was added to a security-enabled universal group
4767	An user account was unlocked
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested.
4770	This event generates for every Ticket Granting Service (TGS) ticket renewal. This event generates only on domain controllers.
4771	Kerberos pre-authentication failed
4772	A Kerberos authentication ticket request failed
4776	The domain controller attempted to validate the credentials for an account
4778	A session was reconnected to a window station
4779	A session was disconnected from a Window Station

4782	The password hash of an account was accessed
4797	Attempt was made to query the existence of a blank password for an account
4797	An attempt was made to query the existence of a blank password for an account
4798	A user's local group membership was enumerated
4799	A security-enabled local group membership was enumerated
4800	The workstation was locked
4801	The workstation was unlocked
4802	Screen saver was invoked
4803	Screen saver was dismissed
4820	A Kerberos Ticket-granting-ticket(TGT) was denied because the device does not meet the access control restrictions
4911	Resource attributes of the object were changed
5140	A network share object was accessed.
5142	A network share object was added.
5144	A network share object was deleted.
5145	A network share object was checked to see whether the client can be granted desired access.
5156	The Windows Filtering Platform has allowed a connection.
5379	Credential Manager credentials were read
6273	Network Policy Server denied access to a user
6276	Network Policy Server quarantined a user
6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6414	New external device
7045	A new service was installed in the system.
8222	Shadow copy has been created.