Time	Event
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=20 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-General Type=Information RecordNumber=1498 Keywords=Time TaskCategory=6 OpCode=Info Message=The leap second configuration has been updated. Reason: Leap second data initialized from registry during boot Leap seconds enabled: true New leap second count: 0 Old leap second count: 0
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=32 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1497 Keywords=None TaskCategory=58 OpCode=Info Message=The bootmgr spent 75935 ms waiting for user input.
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=18 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1496 Keywords=None TaskCategory=57 OpCode=Info Message=There are 0x1 boot options on this system.
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=27 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1495 Keywords=None TaskCategory=33 OpCode=Info Message=The boot type was 0x0.

Time	Event
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=25 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1494 Keywords=None TaskCategory=32 OpCode=Info Message=The boot menu policy was 0x1.
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=20 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1493 Keywords=None TaskCategory=31 OpCode=Info Message=The last shutdown's success status was false. The last boot's success status was true.
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=153 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-Boot Type=Information RecordNumber=1492 Keywords=None TaskCategory=62 OpCode=Info Message=Virtualization-based security (policies: 0) is disabled.
2023-02-17T12:03:58-0800	02/17/2023 12:03:58 PM LogName=System EventCode=12 EventType=4 ComputerName=DESKTOP-64LBDQP User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Kernel-General Type=Information RecordNumber=1491 Keywords=None TaskCategory=1 OpCode=Info Message=The operating system started at system time 2023-02-17T20:03:53.500000000Z.

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74958 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18b0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74957 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe88 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74956 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe88 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74955 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fec Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74954 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1fec New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74953 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18b0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74952 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8cc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74951 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8cc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74950 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a48 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74949 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a48 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74948 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1760 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74947 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1760 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74946 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d50 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74945 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d50 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74944 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x830 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74943 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x830 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:56-0800	02/17/2023 12:03:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74942 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x11fc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:55-0800	02/17/2023 12:03:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74941 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x11fc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74940 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x7a4 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74939 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a54 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74938 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x10b4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74937 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x10b4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a54 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74936 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a54 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74935 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x250 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:52-0800	02/17/2023 12:03:52 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74934 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf14 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74933 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf14 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x250 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74932 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x250 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74931 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fe0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74930 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x11dc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74929 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a98 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74928 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb10 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74927 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xea8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74926 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1984 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74925 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e00 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74924 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12e8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74923 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x11dc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1fe0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74922 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1fe0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74921 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x68c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74920 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f8c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74919 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xea8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xb10 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74918 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb10 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74917 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2148 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74916 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x27c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:51-0800	02/17/2023 12:03:51 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74915 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12e8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1e00 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74914 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e00 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1984 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74913 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1064 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74912 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x21f8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74911 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f8c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x68c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74910 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x68c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74909 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1660 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74908 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d10 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74907 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x27c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2148 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74906 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2148 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74905 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c04 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74904 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1868 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74903 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1890 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74902 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x21f8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1064 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74901 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1064 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1984 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74900 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12fc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74899 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d10 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1660 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74898 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b9c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74897 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1890 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74896 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb2c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74895 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1660 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74894 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b9c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74893 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb2c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:50-0800	02/17/2023 12:03:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74892 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2044 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74891 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1868 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1c04 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74890 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c04 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74889 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12fc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1984 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74888 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d98 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74887 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2044 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7a4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74886 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d98 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74885 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1984 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:49-0800	02/17/2023 12:03:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74884 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x7a4 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:48-0800	02/17/2023 12:03:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74883 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a98 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:47-0800	02/17/2023 12:03:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74882 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x13e8 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0xC000013A

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74881 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x216c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74880 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x216c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74879 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15d4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74878 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15d4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74877 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1aec Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74876 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1aec New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74875 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c68 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74874 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c68 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74873 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d70 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74872 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d70 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74871 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x398 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74870 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x398 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:44-0800	02/17/2023 12:03:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74869 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Process Information: New Process ID:0x18e4 New Process Name:C:\Windows\System32\RuntimeBroker.exe Token Elevation Type:%%1938 Mandatory Label:S-1-16-8192 Creator Process ID:0x344 Creator Process Name:C:\Windows\System32\svchost.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74868 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Process Information: New Process ID:0x608 New Process Name:C:\Windows\System32\backgroundTaskHost.exe Token Elevation Type:%%1938 Mandatory Label:S-1-16-4096 Creator Process ID:0x344 Creator Process Name:C:\Windows\System32\svchost.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74867 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x718 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74866 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ab8 New Process Name:C:\Windows\System32\svchost.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2c4 Creator Process Name:C:\Windows\System32\services.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4670 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74865 Keywords=Audit Success TaskCategory=Authorization Policy Change OpCode=Info Message=Permissions on an object were changed. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Object: Object Server:Security Object Type:Token Object Name:- Handle ID:0x69c Process: Process ID:0x2c4 Process Name:C:\Windows\System32\services.exe Permissions Change: Original Security Descriptor:D:(A;;GA;;;SY)(A;;RCGXGR;;;BA) New Security Descriptor:D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;S-1-5-80-1949724575-2387902436-65106593-1201171665-3967308604)
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74864 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Privileges:SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4627 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74863 Keywords=Audit Success TaskCategory=Group Membership OpCode=Info Message=Group membership information. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:5 New Logon: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Event in sequence:1 of 1 Group Membership: %{S-1-5-32-544} %{S-1-1-0} %{S-1-5-11} %{S-1-16-16384} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74862 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:5 Restricted Admin Mode:- Virtual Account:No Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x2c4 Process Name:C:\Windows\System32\services.exe Network Information: Workstation Name:- Source Network Address:- Source Port:- Detailed Authentication Information: Logon Process:Advapi Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74861 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ab4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74860 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ab4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x718 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:43-0800	02/17/2023 12:03:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74859 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x718 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74858 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ffc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74857 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19ac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74856 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19ac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74855 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9fc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74854 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9fc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74853 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ffc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74852 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xde8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74851 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xde8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74850 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1804 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74849 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x164 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74848 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1804 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74847 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x17d8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74846 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x17d8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74845 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1068 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74844 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1068 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74843 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1680 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74842 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1bdc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74841 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1bdc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1680 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74840 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1680 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:39-0800	02/17/2023 12:03:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74839 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23c0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74838 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1468 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74837 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2104 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74836 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1468 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x23c0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74835 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23c0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74834 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x61c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74833 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1118 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74832 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2168 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74831 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15b8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74830 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d54 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74829 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2168 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x61c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74828 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15b8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1118 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74827 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1118 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2104 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74826 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x61c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74825 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b94 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74824 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xfd8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74823 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1794 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74822 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xcc0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74821 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe78 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:38-0800	02/17/2023 12:03:38 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74820 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x10f0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74819 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1794 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xfd8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74818 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xcc0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1b94 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74817 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xfd8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74816 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b94 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2104 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74815 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x10f0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xe78 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74814 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe78 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d54 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74813 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x125c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74812 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14e8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74811 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1da0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74810 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fe8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74809 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf54 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74808 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b00 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74807 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14e8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x125c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74806 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x125c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2104 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74805 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1fe8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1da0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74804 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1da0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74803 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b00 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xf54 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74802 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x500 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74801 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf54 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d54 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74800 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14d4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:37-0800	02/17/2023 12:03:37 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74799 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2090 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74798 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x500 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74797 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14d4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d54 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74796 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2090 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2104 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74795 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2104 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74794 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x164 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:36-0800	02/17/2023 12:03:36 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74793 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d54 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74792 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2048 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74791 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x13ac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74790 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23ac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74789 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x13ac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74788 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x217c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74787 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x217c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74786 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2048 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74785 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xebc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74784 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b48 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74783 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xebc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74782 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x990 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74781 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b48 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74780 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x990 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74779 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23ac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74778 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x231c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:33-0800	02/17/2023 12:03:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74777 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x231c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74776 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9d8 Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74775 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x130c Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74774 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x177c Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74773 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe5c Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74772 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9d8 New Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74771 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x130c New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74770 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x177c New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:30-0800	02/17/2023 12:03:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74769 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe5c New Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74768 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18b0 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74767 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8cc Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74766 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1758 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74765 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x131c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74764 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe58 Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74763 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x770 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74762 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2280 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74761 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x131c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1758 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74760 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1758 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74759 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8b0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74758 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb68 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74757 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2280 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x770 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74756 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x770 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xe58 Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74755 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe58 New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74754 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x3d0 Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74753 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x99c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:29-0800	02/17/2023 12:03:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74752 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1dcc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74751 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1dac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74750 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1380 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74749 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb68 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8b0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74748 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8b0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74747 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd30 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74746 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d08 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74745 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e28 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74744 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ed4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74743 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x21d0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74742 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c4c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74741 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e38 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74740 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e38 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74739 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d5c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74738 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1dcc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x99c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74737 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d5c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74736 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x4a0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74735 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x99c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x3d0 Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74734 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1dac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74733 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e28 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74732 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x3d0 New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74731 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x4a0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74730 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ed4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74729 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1acc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74728 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x4b0 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74727 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d08 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xd30 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74726 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd30 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74725 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xdcc Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:28-0800	02/17/2023 12:03:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74724 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1180 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74723 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1890 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74722 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1af4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74721 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c4c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x21d0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74720 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x21d0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74719 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1df4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74718 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1310 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74717 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1acc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74716 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1180 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xdcc Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74715 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xdcc New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74714 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1af4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1890 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74713 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1890 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x4b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74712 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1310 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1df4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74711 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1df4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74710 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x111c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74709 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12fc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74708 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1cb4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74707 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2274 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74706 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2008 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:27-0800	02/17/2023 12:03:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74705 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xca0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74704 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x11a4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74703 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14fc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74702 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2274 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1cb4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74701 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12fc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x111c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74700 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1cb4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x4b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74699 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x111c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74698 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x10b0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74697 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xca0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74696 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2008 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74695 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8d0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74694 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x52c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74693 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xc78 Process Name:C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe Exit Status:0x1
2023-02-17T12:03:26-0800	02/17/2023 12:03:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74692 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1420 Process Name:C:\Program Files\Splunk\bin\splunk-admon.exe Exit Status:0x1

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74691 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x10b0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x4b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74690 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14fc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x11a4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74689 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x11a4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18b0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74688 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8d0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8cc Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74687 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xc78 New Process Name:C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74686 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1420 New Process Name:C:\Program Files\Splunk\bin\splunk-admon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:25-0800	02/17/2023 12:03:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74685 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x52c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:24-0800	02/17/2023 12:03:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74684 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x4b0 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:24-0800	02/17/2023 12:03:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74683 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1380 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:24-0800	02/17/2023 12:03:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74682 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8cc New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:24-0800	02/17/2023 12:03:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74681 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18b0 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74680 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19b4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74679 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x21ec Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74678 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19b4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74677 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x21ec New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74676 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d70 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74675 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d70 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74674 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x5b4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74673 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x5b4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74672 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12f4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74671 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12f4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74670 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:22-0800	02/17/2023 12:03:22 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74669 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74668 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23a0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74667 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23a0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74666 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x608 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74665 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x608 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74664 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ae4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74663 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x17a4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74662 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ae4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74661 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x17a4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74660 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xbc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74659 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xbc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74658 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1df8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74657 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1df8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74656 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x224c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:17-0800	02/17/2023 12:03:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74655 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x224c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74654 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f18 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74653 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x20a0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74652 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74651 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x20a0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74650 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x20a0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74649 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14b4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74648 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e1c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74647 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e1c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14b4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74646 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14b4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74645 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f20 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74644 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2b8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74643 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x95c Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74642 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f9c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74641 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22fc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74640 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2b8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f20 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74639 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f20 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74638 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x864 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74637 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a00 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74636 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1970 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74635 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22fc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f9c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74634 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f9c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x95c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74633 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x61c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74632 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x6f8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74631 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x181c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:16-0800	02/17/2023 12:03:16 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74630 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x580 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74629 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a00 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x864 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74628 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x864 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74627 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xfd8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74626 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x6f8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x61c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74625 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd88 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74624 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x61c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x95c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74623 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x580 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x181c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74622 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x181c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1970 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74621 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14ac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74620 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x50c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74619 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b5c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74618 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1438 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74617 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd88 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xfd8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74616 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xfd8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74615 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x678 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74614 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x50c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14ac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74613 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14ac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x95c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74612 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1438 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1b5c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74611 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b5c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1970 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74610 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c5c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74609 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22c8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74608 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x678 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f18 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74607 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c5c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1970 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:15-0800	02/17/2023 12:03:15 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74606 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22c8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x95c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:14-0800	02/17/2023 12:03:14 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74605 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f18 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:14-0800	02/17/2023 12:03:14 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74604 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x95c New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:14-0800	02/17/2023 12:03:14 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74603 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1970 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:12-0800	02/17/2023 12:03:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74602 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x564 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74601 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1714 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74600 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1714 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74599 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x564 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74598 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8ac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74597 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8ac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74596 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23dc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74595 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23dc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74594 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14d4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74593 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14d4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74592 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x134 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74591 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x134 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74590 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12ec Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74589 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12ec New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74588 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf60 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:11-0800	02/17/2023 12:03:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74587 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf60 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74586 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x234c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74585 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fe0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74584 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x172c Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74583 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c08 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74582 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x234c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74581 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c08 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74580 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1988 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74579 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1988 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74578 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1fe0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74577 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9d8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74576 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x130c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74575 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x130c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9d8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74574 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9d8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74573 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74572 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x20f0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74571 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2340 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74570 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb04 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74569 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d50 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74568 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x20f0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1fac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74567 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1fac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74566 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1110 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74565 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x520 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74564 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1848 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74563 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x938 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:06-0800	02/17/2023 12:03:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74562 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe94 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74561 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d50 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xb04 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74560 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb04 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2340 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74559 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12ac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74558 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x175c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74557 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x520 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1110 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74556 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1110 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74555 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x27c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74554 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x99c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74553 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe94 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x938 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74552 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x938 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1848 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74551 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e28 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74550 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12e8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74549 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x175c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x12ac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74548 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12ac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2340 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74547 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x99c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x27c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74546 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x27c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74545 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ed4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74544 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2084 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74543 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xed4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74542 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1090 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74541 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12e8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1e28 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74540 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e28 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1848 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74539 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd78 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74538 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2084 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1ed4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74537 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ed4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2340 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74536 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1090 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xed4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74535 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xed4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74534 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1048 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74533 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a40 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74532 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd78 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1848 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74531 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a40 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x172c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74530 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1048 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2340 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74529 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1848 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:05-0800	02/17/2023 12:03:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74528 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2340 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:04-0800	02/17/2023 12:03:04 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74527 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x172c New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74526 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x990 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74525 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf50 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74524 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf50 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74523 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2378 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74522 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2378 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74521 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x990 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74520 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf58 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74519 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf58 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74518 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1890 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74517 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1890 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74516 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19e4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74515 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19e4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:03:01-0800	02/17/2023 12:03:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74514 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x188c Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:03:00-0800	02/17/2023 12:03:00 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74513 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb14 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:03:00-0800	02/17/2023 12:03:00 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74512 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb14 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x188c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:03:00-0800	02/17/2023 12:03:00 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74511 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x188c New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74510 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x330 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74509 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1310 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74508 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1310 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74507 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a98 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74506 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a98 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74505 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xba4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74504 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xc78 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74503 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xba4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74502 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xc78 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74501 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x52c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74500 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x52c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74499 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x330 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74498 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e80 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74497 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e80 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74496 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8d0 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74495 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a48 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74494 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1524 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74493 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1524 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a48 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74492 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a48 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74491 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e18 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74490 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e68 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74489 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e68 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1e18 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74488 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e18 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74487 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15dc Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74486 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb78 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74485 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1380 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74484 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e78 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:55-0800	02/17/2023 12:02:55 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74483 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1264 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74482 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb78 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15dc Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74481 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15dc New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74480 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x424 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74479 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9d4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74478 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d70 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74477 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1264 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1e78 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74476 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x5e4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74475 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e78 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74474 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xbc Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74473 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22f8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74472 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1014 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74471 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9d4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x424 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74470 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x424 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74469 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x224c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74468 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1014 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xbc Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74467 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22f8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x5e4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74466 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1704 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74465 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xbc New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74464 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x5e4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d70 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74463 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74462 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1604 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74461 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x45c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:54-0800	02/17/2023 12:02:54 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74460 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ce0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74459 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1704 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x224c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74458 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x224c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74457 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1934 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74456 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1604 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74455 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74454 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ce0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x45c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74453 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x45c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d70 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74452 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b70 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74451 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f20 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74450 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1934 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8d0 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74449 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b70 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d70 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74448 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f20 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1380 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74447 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8d0 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74446 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1380 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:53-0800	02/17/2023 12:02:53 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74445 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d70 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:51-0800	02/17/2023 12:02:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74444 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x374 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:50-0800	02/17/2023 12:02:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74443 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x374 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:50-0800	02/17/2023 12:02:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74442 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1898 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:50-0800	02/17/2023 12:02:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74441 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1898 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:50-0800	02/17/2023 12:02:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74440 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19ec Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:50-0800	02/17/2023 12:02:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74439 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19ec New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:47-0800	02/17/2023 12:02:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74438 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x6f8 Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:02:47-0800	02/17/2023 12:02:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74437 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22a0 Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1
2023-02-17T12:02:47-0800	02/17/2023 12:02:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74436 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8dc Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1

Time	Event
2023-02-17T12:02:47-0800	02/17/2023 12:02:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74435 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x6f8 New Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74434 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22a0 New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74433 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a1c Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74432 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8dc New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74431 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a1c New Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74430 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15c8 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74429 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2350 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74428 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x154 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74427 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf54 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74426 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15b0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:46-0800	02/17/2023 12:02:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74425 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1abc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74424 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1be0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74423 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15b8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74422 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14ac Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74421 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd38 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74420 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15b8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74419 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x154 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74418 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2374 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74417 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2350 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74416 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd38 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74415 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1534 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74414 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c5c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74413 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2374 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74412 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15b0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74411 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1534 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74410 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c5c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74409 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1be0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74408 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x66c Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74407 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x164 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74406 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23dc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74405 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1abc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xf54 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74404 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf54 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74403 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x134 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:45-0800	02/17/2023 12:02:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74402 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xc54 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74401 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23dc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x164 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74400 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x164 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x66c Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74399 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x66c New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14ac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74398 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2388 Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74397 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1bf0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74396 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf60 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74395 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xc54 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x134 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74394 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xca8 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74393 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x134 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74392 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2344 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74391 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1870 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74390 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x13ac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:44-0800	02/17/2023 12:02:44 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74389 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1284 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74388 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf60 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1bf0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74387 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1bf0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2388 Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74386 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2388 New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14ac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74385 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1870 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2344 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74384 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2344 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74383 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8c0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74382 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1284 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x13ac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74381 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x10b4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74380 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x13ac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xca8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74379 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x558 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74378 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2280 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74377 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1758 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74376 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x130c Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74375 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x770 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:43-0800	02/17/2023 12:02:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74374 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf24 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74373 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x10b4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8c0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74372 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8c0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74371 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1758 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14ac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74370 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2280 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x558 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74369 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x558 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xca8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74368 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x938 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74367 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d9c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74366 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf24 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x770 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74365 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1dcc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74364 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12ac Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74363 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x770 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x130c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74362 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd44 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:42-0800	02/17/2023 12:02:42 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74361 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c4c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74360 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12ac New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d9c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74359 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d9c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xca8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74358 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1dcc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x938 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74357 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x938 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74356 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e28 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74355 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e00 Process Name:C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe Exit Status:0x1
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74354 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c4c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xd44 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74353 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x294 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74352 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x4f8 Process Name:C:\Program Files\Splunk\bin\splunk-admon.exe Exit Status:0x1

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74351 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd44 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x130c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74350 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x68c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74349 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1acc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:41-0800	02/17/2023 12:02:41 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74348 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x118c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74347 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e00 New Process Name:C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74346 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e28 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x15c8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74345 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x4f8 New Process Name:C:\Program Files\Splunk\bin\splunk-admon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74344 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x294 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xca8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74343 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x118c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x130c Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74342 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1acc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x68c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74341 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x68c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x14ac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:40-0800	02/17/2023 12:02:40 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74340 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2e4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74339 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2074 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74338 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74337 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2074 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74336 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74335 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2e4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74334 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xca8 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74333 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15c8 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74332 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x130c New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:39-0800	02/17/2023 12:02:39 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74331 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14ac New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74330 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xab4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74329 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xab4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74328 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ac0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74327 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ac0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74326 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ae8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74325 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ae8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74324 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1660 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74323 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1660 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74322 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x324 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74321 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x324 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74320 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15d4 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:34-0800	02/17/2023 12:02:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74319 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15d4 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74318 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2008 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74317 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x16e0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74316 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x674 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74315 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1434 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74314 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x144c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74313 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x16e0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74312 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x674 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74311 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1064 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74310 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1064 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74309 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x144c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1434 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74308 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1434 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74307 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xfb0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:29-0800	02/17/2023 12:02:29 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74306 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1760 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74305 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1760 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xfb0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74304 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xfb0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74303 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d64 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74302 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22e8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74301 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1bac Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74300 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x10fc Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74299 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a48 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:28-0800	02/17/2023 12:02:28 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74298 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a98 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74297 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x4d0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74296 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18f8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74295 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22e8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d64 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74294 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d64 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74293 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd84 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74292 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x508 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74291 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a48 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x10fc Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74290 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x10fc New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1bac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74289 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x608 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74288 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19c8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:27-0800	02/17/2023 12:02:27 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74287 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18f8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x4d0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74286 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x4d0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74285 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x508 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xd84 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74284 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd84 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74283 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8e0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74282 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x70c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74281 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xc1c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74280 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2ec Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74279 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19c8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x608 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74278 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x608 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1bac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74277 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f50 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:26-0800	02/17/2023 12:02:26 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74276 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1704 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74275 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x70c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8e0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74274 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8e0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74273 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9fc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74272 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2ec New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xc1c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74271 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xc1c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74270 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14b4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74269 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1704 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1f50 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:25-0800	02/17/2023 12:02:25 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74268 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f50 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1bac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74267 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x17d8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74266 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9fc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a98 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74265 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14b4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2008 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74264 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x17d8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1bac Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74263 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x212c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74262 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb68 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74261 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b00 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74260 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22dc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74259 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x212c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74258 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22dc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:24-0800	02/17/2023 12:02:24 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74257 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb68 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74256 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b00 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74255 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2b8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74254 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2384 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74253 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x13f8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74252 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2b8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74251 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2384 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74250 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x13f8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74249 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a98 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74248 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2008 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:23-0800	02/17/2023 12:02:23 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74247 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1bac New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74246 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x308 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74245 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x308 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74244 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1cb0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74243 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1cb0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74242 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22fc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:17-0800	02/17/2023 12:02:17 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74241 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22fc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:13-0800	02/17/2023 12:02:13 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74240 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d04 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74239 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d04 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74238 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xcc0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74237 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xcc0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74236 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1da8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74235 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1da8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74234 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1934 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74233 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1934 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74232 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19c0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74231 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19c0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:12-0800	02/17/2023 12:02:12 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74230 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x354 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74229 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x354 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74228 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1074 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74227 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1074 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74226 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x50c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74225 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x50c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74224 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1cc8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74223 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1cc8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74222 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb44 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74221 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x580 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74220 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c7c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74219 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1914 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74218 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c20 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74217 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x950 New Process Name:C:\Windows\System32\SearchFilterHost.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-8192 Creator Process ID:0x18b4 Creator Process Name:C:\Windows\System32\SearchIndexer.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4670 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74216 Keywords=Audit Success TaskCategory=Authorization Policy Change OpCode=Info Message=Permissions on an object were changed. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Object: Object Server:Security Object Type:Token Object Name:- Handle ID:0xcc0 Process: Process ID:0x18b4 Process Name:C:\Windows\System32\SearchIndexer.exe Permissions Change: Original Security Descriptor: D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;S-1-5-80-117416528-2204451360-1913602512-1355018040-1234992034)(A;;GA;;;BA) New Security Descriptor: D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;S-1-5-80-117416528-2204451360-1913602512-1355018040-1234992034)(A;;GA;;;BA)(A;;SWRPRC;;;S-1-5-5-0-606737)
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4670 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74215 Keywords=Audit Success TaskCategory=Authorization Policy Change OpCode=Info Message=Permissions on an object were changed. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Object: Object Server:Security Object Type:Token Object Name:- Handle ID:0xdb8 Process: Process ID:0x18b4 Process Name:C:\Windows\System32\SearchIndexer.exe Permissions Change: Original Security Descriptor:D:(A;;GA;;;S-1-5-21-1967644673-3160760465-3523697353-1001)(A;;GA;;;SY)(A;;GXGR;;;S-1-5-5-0-21090276) New Security Descriptor: D:(A;;GA;;;S-1-5-21-1967644673-3160760465-3523697353-1001)(A;;GA;;;SY)(A;;GXGR;;;S-1-5-5-0-21090276)(A;;GA;;;BA)

Time	Event
2023-02-17T12:02:11-0800	02/17/2023 12:02:11 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74214 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Process Information: New Process ID:0x1d58 New Process Name:C:\Windows\System32\SearchProtocolHost.exe Token Elevation Type:%%1938 Mandatory Label:S-1-16-8192 Creator Process ID:0x18b4 Creator Process Name:C:\Windows\System32\SearchIndexer.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:10-0800	02/17/2023 12:02:10 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74213 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c7c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xb44 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:10-0800	02/17/2023 12:02:10 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74212 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c20 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1914 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:10-0800	02/17/2023 12:02:10 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74211 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1914 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:10-0800	02/17/2023 12:02:10 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74210 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d3c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:10-0800	02/17/2023 12:02:10 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74209 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15e0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74208 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1480 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74207 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1030 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74206 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x17ec Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74205 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb44 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74204 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15e0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d3c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74203 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d3c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74202 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x217c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:09-0800	02/17/2023 12:02:09 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74201 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x458 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74200 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x17ec New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1030 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74199 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1030 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1480 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74198 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1284 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74197 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1458 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74196 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x974 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74195 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x458 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x217c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74194 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x217c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74193 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x84c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74192 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf70 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74191 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c60 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74190 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d34 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74189 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x320 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:08-0800	02/17/2023 12:02:08 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74188 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1458 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1284 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74187 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1284 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1480 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74186 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a1c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74185 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x8b0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74184 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b98 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74183 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1a1c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74182 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf70 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x84c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74181 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x84c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74180 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x320 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74179 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d34 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1c60 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74178 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c60 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x974 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74177 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x99c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74176 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xb1c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74175 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1dac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:02:07-0800	02/17/2023 12:02:07 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74174 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1dcc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74173 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b98 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x8b0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74172 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x8b0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1480 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74171 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xb1c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x99c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74170 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x99c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74169 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1dcc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1dac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74168 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf14 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74167 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1dac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x974 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74166 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ed4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:06-0800	02/17/2023 12:02:06 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74165 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2298 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:02:05-0800	02/17/2023 12:02:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74164 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf14 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x580 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:05-0800	02/17/2023 12:02:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74163 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ed4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x974 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:05-0800	02/17/2023 12:02:05 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74162 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2298 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1480 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:04-0800	02/17/2023 12:02:04 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74161 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1480 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:04-0800	02/17/2023 12:02:04 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74160 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x580 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:04-0800	02/17/2023 12:02:04 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74159 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x974 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74158 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x88c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74157 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1330 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74156 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1330 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74155 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c04 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74154 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c04 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:02:02-0800	02/17/2023 12:02:02 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74153 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x88c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:02:01-0800	02/17/2023 12:02:01 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74152 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x15cc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:02:00-0800	02/17/2023 12:02:00 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74151 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x15cc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x13e8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74150 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd78 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74149 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x294 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74148 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x294 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74147 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x107c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74146 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd78 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74145 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x107c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:59-0800	02/17/2023 12:01:59 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74144 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x13e8 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74143 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74142 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74141 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-21-1967644673-3160760465-3523697353-1001 Account Name:Jackson Yuan Account Domain:DESKTOP-64LBDQP Logon ID:0x141D16A Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74140 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74139 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=5379 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74138 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=Credential Manager credentials were read. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Read Operation:Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74137 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x244 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74136 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x192c New Process Name:C:\Windows\System32\svchost.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2c4 Creator Process Name:C:\Windows\System32\services.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4670 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74135 Keywords=Audit Success TaskCategory=Authorization Policy Change OpCode=Info Message=Permissions on an object were changed. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Object: Object Server:Security Object Type:Token Object Name:- Handle ID:0x3b8 Process: Process ID:0x2c4 Process Name:C:\Windows\System32\services.exe Permissions Change: Original Security Descriptor:D:(A;;GA;;;SY)(A;;RCGXGR;;;BA) New Security Descriptor:D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;S-1-5-80-2952724807-2252311773-3412998076-2712868122-780978283)
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74134 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Privileges:SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4627 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74133 Keywords=Audit Success TaskCategory=Group Membership OpCode=Info Message=Group membership information. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:5 New Logon: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Event in sequence:1 of 1 Group Membership: %{S-1-5-32-544} %{S-1-1-0} %{S-1-5-11} %{S-1-16-16384} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74132 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:5 Restricted Admin Mode:- Virtual Account:No Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-18 Account Name:SYSTEM Account Domain:NT AUTHORITY Logon ID:0x3E7 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x2c4 Process Name:C:\Windows\System32\services.exe Network Information: Workstation Name:- Source Network Address:- Source Port:- Detailed Authentication Information: Logon Process:Advapi Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74131 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x244 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74130 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xaac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74129 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xaac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74128 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c6c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:56-0800	02/17/2023 12:01:56 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74127 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c6c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:53-0800	02/17/2023 12:01:53 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74126 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14f4 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x72

Time	Event
2023-02-17T12:01:51-0800	02/17/2023 12:01:51 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74125 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe58 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74124 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xef8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74123 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xef8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74122 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x12fc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74121 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe58 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74120 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x12fc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74119 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2300 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:50-0800	02/17/2023 12:01:50 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74118 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2300 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74117 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x9f4 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74116 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ba8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74115 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x47c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74114 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x47c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1ba8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74113 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ba8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74112 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1224 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:49-0800	02/17/2023 12:01:49 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74111 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x444 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74110 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x444 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1224 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74109 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1224 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74108 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xfb0 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74107 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e68 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74106 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x704 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74105 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2034 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74104 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1be8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:48-0800	02/17/2023 12:01:48 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74103 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1434 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74102 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x142c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74101 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f3c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74100 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e68 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xfb0 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74099 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xfb0 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74098 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18e4 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74097 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x229c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74096 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1be8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x2034 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74095 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2034 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x704 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74094 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18a8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74093 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x780 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74092 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f3c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x142c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:47-0800	02/17/2023 12:01:47 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74091 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x142c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1434 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74090 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x229c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18e4 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74089 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18e4 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74088 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1604 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74087 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f94 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74086 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1df8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74085 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22f8 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74084 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x780 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18a8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74083 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18a8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x704 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74082 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1aac Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74081 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x16bc Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74080 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f94 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1604 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74079 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1604 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1434 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:46-0800	02/17/2023 12:01:46 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74078 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1f50 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74077 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1eac Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74076 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22f8 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1df8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74075 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2044 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74074 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ed0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74073 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1bdc Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74072 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1eac New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74071 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1df8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74070 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1bdc New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74069 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ed0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74068 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2044 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74067 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23c0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74066 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x16bc New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1aac Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74065 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1aac New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x704 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74064 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1588 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74063 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1f50 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1434 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:45-0800	02/17/2023 12:01:45 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74062 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23c0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x9f4 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:44-0800	02/17/2023 12:01:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74061 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1588 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x704 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:44-0800	02/17/2023 12:01:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74060 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1434 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:44-0800	02/17/2023 12:01:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74059 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9f4 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:44-0800	02/17/2023 12:01:44 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74058 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x704 New Process Name:C:\Program Files\Splunk\bin\python3.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74057 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xf3c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74056 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1e1c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74055 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1e1c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74054 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x154c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74053 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x154c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:43-0800	02/17/2023 12:01:43 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74052 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xf3c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74051 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1028 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74050 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1028 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74049 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1688 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74048 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1688 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74047 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2008 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:40-0800	02/17/2023 12:01:40 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74046 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2008 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:36-0800	02/17/2023 12:01:36 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74045 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xab8 Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74044 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1aa0 Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74043 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2168 Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Exit Status:0x1

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74042 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xab8 New Process Name:C:\Program Files\Splunk\bin\splunk-regmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74041 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1aa0 New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74040 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2168 New Process Name:C:\Program Files\Splunk\bin\splunk-powershell.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74039 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x19c Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74038 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1ad0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74037 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1ad0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74036 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x19c New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74035 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe78 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74034 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xe78 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74033 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c28 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:35-0800	02/17/2023 12:01:35 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74032 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c28 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74031 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x61c Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Exit Status:0x1

Time	Event
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74030 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1fe8 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74029 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d04 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74028 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1cc8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74027 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d10 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74026 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x61c New Process Name:C:\Program Files\Splunk\bin\splunk-netmon.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74025 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xfb4 Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74024 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1950 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:34-0800	02/17/2023 12:01:34 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74023 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1684 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74022 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d10 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1cc8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74021 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1cc8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d04 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74020 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x7c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74019 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x14d4 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74018 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1684 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1950 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74017 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1950 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xfb4 Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74016 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xfb4 New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1fe8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74015 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c5c Process Name:C:\Program Files\Splunk\bin\splunk.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74014 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b5c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74013 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x62c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74012 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1318 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74011 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x930 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:33-0800	02/17/2023 12:01:33 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74010 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23d0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74009 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x14d4 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x7c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74008 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x7c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d04 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74007 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d74 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74006 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x17ec Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74005 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x62c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1b5c Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74004 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b5c New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1c5c Creator Process Name:C:\Program Files\Splunk\bin\splunk.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74003 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1c5c New Process Name:C:\Program Files\Splunk\bin\splunk.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1fe8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74002 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xa34 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74001 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23d0 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x930 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=74000 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x930 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1318 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73999 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x18ec Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73998 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x139c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73997 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x17ec New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d74 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73996 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xc50 Process Name:C:\Program Files\Splunk\bin\python3.exe Exit Status:0x0
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73995 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d74 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d04 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73994 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1d18 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:32-0800	02/17/2023 12:01:32 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73993 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x23ac Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73992 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x22b8 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73991 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x217c Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73990 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x2324 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73989 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b94 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73988 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xa34 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1fe8 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73987 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1da8 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73986 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1da8 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73985 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b94 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73984 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1b88 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73983 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x16f0 Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Exit Status:0x0
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73982 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2324 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73981 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x16f0 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:31-0800	02/17/2023 12:01:31 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73980 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1b88 New Process Name:C:\Program Files\Splunk\bin\splunk-optimize.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x215c Creator Process Name:C:\Program Files\Splunk\bin\splunkd.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73979 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x139c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x18ec Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73978 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x23ac New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d18 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73977 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x18ec New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1318 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73976 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x1d18 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1d04 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73975 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x217c New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x22b8 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73974 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x22b8 New Process Name:C:\Program Files\Splunk\bin\btool.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0xc50 Creator Process Name:C:\Program Files\Splunk\bin\python3.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73973 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xe5c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73972 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1808 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73971 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1a54 Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73970 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0xd44 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73969 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x1c4c Process Name:C:\Program Files\Splunk\bin\btool.exe Exit Status:0x0
2023-02-17T12:01:30-0800	02/17/2023 12:01:30 PM LogName=Security EventCode=4689 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73968 Keywords=Audit Success TaskCategory=Process Termination OpCode=Info Message=A process has exited. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:0x21d0 Process Name:C:\Program Files\Splunk\bin\splunkd.exe Exit Status:0x0

Time	Event
2023-02-17T12:01:29-0800	02/17/2023 12:01:29 PM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-64LBDQP SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=73967 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:DESKTOP-64LBDQP$ Account Domain:WORKGROUP Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0xd44 New Process Name:C:\Program Files\Splunk\bin\splunkd.exe Token Elevation Type:%%1936 Mandatory Label:S-1-16-16384 Creator Process ID:0x1a54 Creator Process Name:C:\Program Files\Splunk\bin\btool.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.